

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

SYNOPSYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., et al.,

Defendants.

Case No. [17-cv-00561-WHO](#)

**ORDER ON PENDING MOTIONS**

Re: Dkt. Nos. 34, 35, 54

This case stems from the purported interest of defendants Ubiquiti Network Inc., UNIL, and Ching-Han Tsai to review and evaluate for licensing plaintiff Synopsys, Inc.'s high-value semiconductor electronic design and automation software. Synopsys alleges that defendants fraudulently gained access to their copyrighted software and related support materials and used the evaluation license keys and counterfeit keys to repeatedly and illegally access and copy those programs and materials over the course of three years. When defendants' alleged conduct was discovered, Synopsys sued. Ubiquiti and Tsai seek to dismiss six of seven causes of action in the Amended Complaint (AC), and to strike Synopsys' affirmative defenses to Ubiquiti's counterclaims for declaratory judgment and breach of contract. Separately UNIL moves to dismiss for lack of personal jurisdiction.

For the reasons discussed below, Ubiquiti's motion to dismiss is granted only with respect to the Anti-Counterfeiting Act claim (18 U.S.C. § 2318) and some of the predicate acts alleged under the Racketeer Influenced and Corrupt Organizations Act (RICO, 18 U.S.C. § 1964). I deny Ubiquiti's motion to strike the affirmative defenses in large part because Synopsys has alleged sufficient facts in its AC and Answer to support its defenses and allow Ubiquiti to contest them. I deny UNIL's motion to dismiss for lack of jurisdiction because there are sufficient uncontested facts showing that its conduct has a substantial connection with California.

## BACKGROUND

### I. THE PARTIES

Synopsys is a corporation with a principal place of business in Mountain View, California. AC ¶ 1. It is a leading provider of electronic design automation (EDA) solutions for the semiconductor industry. *Id.* ¶ 22.<sup>1</sup> It has developed a “comprehensive, integrated portfolio of prototyping, IP, implementation, verification, manufacturing, optical, field-programmable gate array, and software quality and security solutions.” *Id.* ¶ 23. Its software applications – including Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi – are works subject to copyright protection. *Id.* ¶ 24. It licenses its software programs to users, using a “License Key” system to provide customers access to the applications *Id.* ¶¶ 25-26.

Ubiquiti Networks Inc. is a corporation headquartered in San Jose, California. AC ¶ 2. It and its subsidiaries “develop high performance networking technology for service providers and enterprises.” AC ¶ 3. A significant part of Ubiquiti’s research and development operations are based outside the United States. *Id.* ¶ 5. Defendant Ubiquiti Networks International, Ltd. (UNIL) is alleged to be a subsidiary of Ubiquiti that is involved in the development and distribution of networking technology for Ubiquiti. *Id.* ¶ 6. UNIL incorporated under the laws of Hong Kong, and has a branch in Taipei, Taiwan. *Id.* Synopsys alleges that Ubiquiti and UNIL share at least one corporate officer, Robert J. Pera. *Id.* ¶ 7. UNIL’s Taipei branch employs persons in the field of semi-conductor design and it regularly conducts semiconductor design activities and designs products to be imported and sold in the United States. *Id.* ¶¶ 8-9. Defendant Ching-Han Tsai is employed by Ubiquiti as a project lead and is a semiconductor professional who regularly works in California. *Id.* ¶¶ 10-13.

### II. THE INCEPTION OF THE PARTIES’ RELATIONSHIP

Synopsys alleges that in 2013 Tsai, Ubiquiti, and UNIL fraudulently induced Synopsys to grant them access to a subset of Synopsys’ software for a finite time for purposes of evaluation.

---

<sup>1</sup> EDA generally refers to using computers to design, verify, and simulate the performance of electronic circuits.

AC ¶ 27. Since 2014, Tsai, Ubiquiti, and UNIL have been “secretly using counterfeit keys” obtained or created through hacker websites to circumvent the License Key system and use Synopsys’ EDA software including its Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi applications without a “valid license.” *Id.* ¶ 28. Synopsys alleges that Tsai and others at Ubiquiti and UNIL “conspired to, and did, form an associated in fact enterprise (‘Piracy Enterprise’) with the purpose of pirating Synopsys’ software and that the defendants took wrongful acts in furtherance of their Enterprise,” including (i) gaining unauthorized access to, (ii) making and distributing copies of, and (iii) using counterfeit keys to make unauthorized use of Synopsys’ software and documentation. *Id.* ¶ 29. It asserts that Ubiquiti and UNIL share information technology structures (communication networks, file repositories, email servers, IP addresses, and website domains hosted in the United States) that were used by both Ubiquiti and UNIL to conduct the Piracy Enterprise. FAC ¶ 30. All three defendants also used interstate internet communications to conduct the Enterprise, including extensive use of the counterfeit License Keys. *Id.* ¶¶ 31-32.

On September 11, 2013, Tsai, acting on behalf of Ubiquiti and UNIL, exchanged emails with Synopsys employees in Mountain View, California, stating that Ubiquiti was interested in licensing Synopsys’ VCS and Verdi EDA software applications, as well as licensing a “separate suite” of semiconductor design materials. AC ¶ 35. On September 12, 2013, Tsai met with Synopsys employees in San Jose and indicated Ubiquiti was also interested in Synopsys’ Design Compiler application. *Id.* Tsai represented that Ubiquiti planned to build a semiconductor design team at Ubiquiti’s U.S. headquarters and that Synopsys was its main choice for EDA software. *Id.* These statements, according to Synopsys, were designed to create the impression that Ubiquiti wanted to create a significant business relationship with Synopsys, but were false when they were made. *Id.*

On September 30, 2013, acting on behalf of the Enterprise, Tsai emailed Synopsys and said that Ubiquiti was interested in taking 21 licenses for various EDA applications during various points from November 2013 through June 2014. *Id.* ¶ 36. On October 1, 2013, Tsai indicated the

1 Ubiquiti wanted to take a local area network (LAN) form of license to be used by a small U.S.  
2 team. *Id.* ¶ 37. On October 14, 2013, Tsai indicated that Ubiquiti intended to make its first EDA  
3 software purchase before October 31, 2013, and that it would prefer to pay Synopsys from an  
4 “offshore account” in Hong Kong. *Id.* ¶ 38. That same day, Tsai also asked by email for an  
5 “evaluation license” for Synopsys’ VCS application, stating that he would be the “one doing the  
6 eval” on his personal laptop. *Id.* ¶ 39. Synopsys alleges that all of these representations were false  
7 when made.

8 On October 15, 2013, in reliance on Tsai’s false representations, Synopsys entered into a  
9 Master Non-Disclosure Agreement (MNDA), the purpose of which was to facilitate the parties’  
10 discussions and potential business relationship. Ubiquiti signed the MNDA on October 15, 2013  
11 and Synopsys executed it on November 25, 2013. *Id.* ¶ 40. From October 14, 2013 through  
12 November 25, 2013, Tsai continued to represent that Ubiquiti was interested in licensing  
13 Synopsys’ EDA tools. Eventually, Tsai negotiated an agreement under which Ubiquiti would  
14 evaluate Synopsys’ VCS application at a specific location in San Jose for 90 days. *Id.* ¶ 41.

15 In reliance on Tsai’s representations, on November 26, 2013, Synopsys executed a 90-day  
16 evaluation license (License) that permitted Ubiquiti to evaluate Synopsys’ VCS application. *Id.* ¶  
17 43. That non-transferable license allowed Ubiquiti to test VCS on two computers in San Jose. *Id.*  
18 The License strictly circumscribed use and prohibited Ubiquiti from using the software to design  
19 products and from “making unauthorized copies of Synopsys’ software, decompiling or reverse  
20 engineering Synopsys’ software, tampering with or attempting to circumvent Synopsys’ license  
21 key system, or distributing Synopsys’ software to third parties, among other restrictions.” *Id.* The  
22 License contained a confidentiality provision and a clause expressly superseding all prior  
23 agreements between the parties “with respect to the subject matter” of the license. *Id.* In order to  
24 facilitate use of the License, Synopsys also provided Tsai with temporary log in credentials  
25 permitting access to Synopsys’ file download and customer service websites that were all located  
26 and hosted in the Northern District (except for one server located in Ireland that was accessed by  
27 the Enterprise through a remote host located in Mountain View, California). *Id.* ¶ 44.

28 Synopsys alleges that Tsai failed to disclose that the Piracy Enterprise intended to use

1 pirated copies of the VCS application at unauthorized locations on unauthorized computers. *Id.*  
2 Shortly after inducing Synopsys to provide the evaluation License, persons acting on behalf of the  
3 Enterprise began using counterfeit license keys to access unauthorized copies of VCS from  
4 unauthorized locations. *Id.* ¶ 42. As soon as Tsai had access to it, Tsai accessed Synopsys’ file  
5 download and customer support website and the Enterprise began making and distributing  
6 unauthorized copies of Synopsys software and documentation using both illicit license keys and  
7 counterfeit facsimiles of Synopsys’ license keys. *Id.* ¶¶ 44, 45. The Enterprise participants – Tsai,  
8 Ubiquiti, and UNIL – passed to one another software and other technology components designed  
9 to circumvent Synopsys’ measures to control access to its copyrighted works. *Id.* ¶ 42.

10 On December 2, 2013, Tsai on behalf of the Enterprise emailed Synopsys that he was  
11 having trouble running the software using the temporary license key, purportedly on a “virtual  
12 machine” located at Ubiquiti’s San Jose headquarters. *Id.* ¶ 46. Synopsys responded and provided  
13 information on how to configure the license key file. *Id.* On the same day, Tsai emailed a  
14 Synopsys employee asking that the Host ID listed in the temporary key file be switched to a new  
15 computer because the prior Host ID was incorrect. *Id.* These representations were false and Tsai  
16 intended to gain new information and access so that the Enterprise could continue its purpose to  
17 run Synopsys software on unauthorized computers in unauthorized locations. *Id.* ¶ 47.

### 18 **III. UNIL’S PARTICIPATION**

19 Synopsys alleges that Ubiquiti and UNIL share information technology structures  
20 (communication networks, file repositories, email servers, IP addresses, and website domains  
21 hosted in the United States) that were used by both Ubiquiti and UNIL to conduct the Piracy  
22 Enterprise. FAC ¶ 30. All three defendants also used interstate internet communications to  
23 conduct the Enterprise, including extensive use of the counterfeit license keys. *Id.* ¶¶ 31-32. In  
24 late 2013 and early 2014, Tsai and others transferred some or all of the files downloaded from  
25 Synopsys to one or more computers controlled by UNIL via Ubiquiti’s and UNIL’s shared IT  
26 infrastructure. *Id.* ¶ 48. In early March 2014, while physically located in the Northern District of  
27 California, Tsai communicated by email to Synopsys about UNIL’s desire to evaluate Synopsys  
28 software and get temporary evaluation licenses for UNIL, falsely indicating UNIL was close to

1 obtaining software from a Synopsys competitor and wanted to evaluate Synopsys' software first.  
2 *Id.* ¶ 49. Included on those emails were UNIL employees who work in semiconductor design. *Id.*

3 In early April 2014, Tsai travelled to Taiwan to help coordinate meetings between UNIL  
4 and Synopsys to discuss UNIL's purported desire to evaluate and license Synopsys' software. *Id.*  
5 ¶ 50. At an April 8, 2014 meeting in Taiwan, Tsai and others represented that UNIL needed quick  
6 access to temporary license keys so that it could evaluate the EDA software before making a  
7 decision. *Id.* Time was of the essence due to UNIL's negotiations with the Synopsys competitor  
8 and the deadlines for a UNIL project. *Id.*

9 All of these representations were false, and made for the purpose of furthering the Piracy  
10 Enterprise. *Id.* ¶ 51. Based on the false representations, on April 14, April 15, and May 9, 2014,  
11 Synopsys provided UNIL temporary license keys for Synopsys' Formality, DC Ultra, HDL  
12 Compiler Verilog, and DesignWare Library applications, as well as its Power Compiler  
13 application. *Id.* ¶ 52. All of the temporary keys allowed for only one or two concurrently running  
14 executions, and all keys were designated to be hosted by licensed servers running only on specific  
15 computers with Host IDs, and would expire in two to four weeks. *Id.* UNIL downloaded  
16 Ubiquiti's software and related documentation and installer files on April 16, 2014 and May 19,  
17 2014. *Id.* ¶ 53. These files were downloaded from servers in Mountain View or through a remote  
18 host located in Mountain View. *Id.* On April 16 and 17, 2014, despite having access to temporary  
19 license keys, UNIL employees began using counterfeit license keys to access Design Compiler  
20 software downloaded by UNIL. *Id.* ¶ 54. On May 19, 2014, a UNIL employee contacted  
21 Synopsys' customer support via email seeking assistance for the use of tools that (not known at  
22 the time to Synopsys) were secretly being copied and used without authorization by the Enterprise,  
23 explaining that access was of the essence because of UNIL's deadline to make a software decision.  
24 *Id.* ¶ 55. Based upon these false representations, and in conjunction with communications with  
25 both Ubiquiti and UNIL personnel, Synopsys provided "work around" solutions, allowing further  
26 access to Synopsys software and documentation. *Id.*

27 Synopsys alleges that there is personal jurisdiction over UNIL in this court because UNIL  
28 "expressly assented" to jurisdiction here by "assenting to Synopsys' websites' terms of use in

order to gain access to copyright-protected software and documentation hosted on Synopsys' file download website." AC ¶ 17. Synopsys also states that UNIL committed a substantial part of the wrongful acts giving rise to this suit within the Northern District, including:

UNIL knowingly and with the intent to make and distribute unauthorized copies downloaded software and documentation from Synopsys servers located in California and the Northern District, carried out business negotiations regarding the software at issue with Synopsys employees located in California, and Tsai, while physically present in California and acting on behalf of UNIL, misrepresented and omitted material facts to Synopsys in order to induce Synopsys to provide UNIL with access to Synopsys' copyright-protected software and documentation.

AC ¶ 18. UNIL is also alleged to have conducted "regular business" within and directed toward California and UNIL's semiconductor design activities are "directed and funded" from Ubiquiti's headquarters in Northern California, by Pera and Tsai among others. *Id.* ¶ 19.

In support of its motion contesting personal jurisdiction, UNIL relies on a declaration from defendant Ching-Han Tsai, a Ubiquiti employee. Dkt. No. 35-1. Tsai declares that he has never been a UNIL employee. Tsai Decl. ¶ 1.<sup>2</sup> Tsai confirms that when he was negotiating with Synopsys to be able to use additional evaluation software in early March 2014, UNIL employees were included on his emails with Synopsys and the "evaluation was to take place in Taiwan." *Id.* ¶ 7. To the best of Tsai's knowledge, no UNIL employees communicated with California-based Synopsys employees but only with "Synopsys Taiwan" employees located in Taiwan. *Id.*

Tsai also asserts that at the April 8, 2014 meeting he attended in Taiwan with UNIL employees, the only Synopsys employees who attended were "Synopsys Taiwan" employees

---

<sup>2</sup> In his declaration, Tsai includes facts that are not relevant to the motion to dismiss for lack of jurisdiction, including his downloading of Synopsys software from Synopsys' sites and that he does not recall ever agreeing to any terms of use on those sites. Tsai Decl. ¶¶ 4, 11. Those facts cannot be relied on to support the 12(b)(6) motion to dismiss. Synopsys makes a number of evidentiary objections to Tsai's declaration, primarily based on the fact that Tsai admits he is not a UNIL employee and, therefore, cannot have personal knowledge of what UNIL did. *Oppo.* 13. The other objections are that the statements are speculative, lack foundation, lack relevance, and are hearsay. *Id.* 13-14. The objections based on speculation, lack of foundation, and lack of relevance are **OVERRULED**. The objections based on hearsay to emails which have not been produced are **SUSTAINED**. While some of the challenged statements could fall within FRE 801(d) or 803(3), that cannot be determined based simply on Tsai's assertion of what the unproduced emails say.

based in Taiwan. *Id.* ¶ 9. Further meetings were held between Tsai, UNIL employees, and the two “Synopsys Taiwan” employees Tony Huang and Victor Chen in early May 2014. *Id.* ¶ 10.

Tsai confirms that while a UNIL employee exchanged emails with a Synopsys Taiwan employee and a Synopsys California-based employee on May 19, 2014, the California-based employee was at the time in Taiwan. *Id.* ¶ 12. To Tsai’s knowledge, no UNIL employee “knowingly interacted” with any Synopsys customer service support personnel located in California. *Id.*

In support of its Reply, UNIL submits a second declaration from Tsai and a declaration from Ubiquiti employee Sheng-Feng Wang. Dkt. Nos. 50-1, 56.<sup>3</sup> According to those declarations, Wang and Tsai are the only two California-based Ubiquiti employees that worked on semiconductor chip design activities with employees of UNIL during the relevant time frame. Wang Decl. ¶ 2; Tsai Reply Decl. ¶ 2. “While present in California,” neither Wang nor Tsai ever received from a UNIL employee a “transmission” containing any unauthorized license keys or unauthorized copies of Synopsys software. Wang Decl. ¶ 3; Tsai Reply Decl. ¶ 3. To the best of their knowledge, “no UNIL employee transmitted to any Ubiquiti employee in California unauthorized license keys or unauthorized copies of Synopsys’ software” in the early March timeframe. Wang Decl. ¶ 3; Tsai Reply Decl. ¶ 3.

#### **IV. PIRACY ENTERPRISE CONDUCT AND SYNOPSIS’ DISCOVERY OF IT**

Synopsys alleges that the volume and nature of the counterfeit keys used by the Enterprise indicates that counterfeit key generation software was used and shared across Ubiquiti’s and UNIL’s shared IT infrastructure. AC ¶¶ 57, 59. Nature and use patterns of the keys also indicate that members of the Enterprise distributed amongst themselves the counterfeit license keys and/or

---

<sup>3</sup> Synopsys objects to the Reply Declarations on the grounds that they address matters that should have been raised in the opening motion, and objects to discrete portions of those declarations as lacking in foundation, speculative, impermissible legal conclusion, impermissible lay opinion, and hearsay. Dkt. No. 53. I will not strike the declarations (although I agree they address subject matters that were called for in support of the motion, if at all) and **OVERRULE** the objections based on impermissible legal and lay opinion, speculation, lack of foundation, and lack of relevance. As to the hearsay objection, that is **SUSTAINED**. However, I will assume for purposes of ruling on this motion that Tony Huang and Victor Chen are based in Taiwan (as Tsai asserts). Those facts, however, are not determinative for UNIL’s motion.



the software to make them in order to permit employees of Ubiquiti and UNIL to access Synopsys’ software and resources without authorization. *Id.* ¶ 58. The Enterprise configured its computers to operate in various modes to allow counterfeit keys to be run off of and/or on multiple remote systems, virtual computers, and across various file paths. *Id.* ¶¶ 60-63. The Enterprise’s counterfeit license key use is “associated” with at least 15 names, some of which correspond to the names of Ubiquiti and UNIL employees. *Id.* ¶ 64.

Synopsys discovered the use of counterfeit keys – at least 39,000 times by Ubiquiti, UNIL, and others, and 66 times by Tsai personally, AC ¶ 32 – in March 2016. *Id.* ¶ 65. Synopsys investigated and in May 2016, issued a cease and desist notice to Ubiquiti, although the Enterprise continued to access Synopsys’ software even after the cease and desist was served. *Id.* ¶ 28.

#### **V. THIS CASE**

Based on these allegations, Synopsys alleged seven causes of action: (1) violation of the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1201(a)(1); (2) violation of the DMCA, 17 U.S.C. § 1201(a)(2); (3) violation of the DMCA, 17 U.S.C. § 1201(b); (4) violation of 18 U.S.C. 2318; (5) fraud; (6) violation of Civil RICO, 18 U.S.C. § 1964; and (7) negligent misrepresentation. Ubiquiti moves to dismiss causes of action 2 through 7 for failure to state a claim. UNIL separately moves to dismiss all of the claims asserted against it for lack of personal jurisdiction.

Ubiquiti and Tsai also filed counterclaims against Synopsys for declaratory judgment and breach of contract. Ubiquiti Answer and Counterclaims [Dkt. No. 19]. The declaratory relief counterclaim seeks a “declaration that the mere use or access of Plaintiff’s software applications, without, separate from, or subsequent to the alleged use of ‘counterfeit’ license keys, does not constitute an act of circumvention under 17 U.S.C. § 1201.” *Id.* 9-10. The breach of contract counterclaim is based on allegations that Synopsys violated the terms of the companies’ Master Non-Disclosure Agreement (MNDA) when two “software monitoring companies” obtained and transmitted confidential Ubiquiti information to Synopsys as a result of monitoring software that was concealed in the software Synopsys provided to Ubiquiti. Answer and Counterclaim ¶¶ 7-11, 18-20. The confidential information obtained and transmitted included “the IP (Internet protocol)

address associated with users’ computers, user names, and other workstation information of Ubiquiti employees, the particular programs and features accessed by each user, and other proprietary and sensitive information belonging to Ubiquiti.” *Id.* ¶ 20.

In its Amended Answer, Synopsys asserts the following affirmative defenses to the counterclaims: (1) fraud; (2) unclean hands; (3) waiver; (4) laches; (5) estoppel; (6) failure to mitigate damages; (7) unjust enrichment; (8) novation; and (9) mistake. Synopsys Amended Answer [Dkt. No. 37]. Ubiquiti moves to strike those affirmative defenses, arguing that they are not adequately alleged or cannot constitute affirmative defenses. Dkt. No. 54.

## LEGAL STANDARD

### I. MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss if a claim fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, the claimant must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when the plaintiff pleads facts that “allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). There must be “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* While courts do not require “heightened fact pleading of specifics,” a claim must be supported by facts sufficient to “raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555, 570.

Under Federal Rule of Civil Procedure 9(b), a party must “state with particularity the circumstances constituting fraud or mistake,” including “the who, what, when, where, and how of the misconduct charged.” *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (internal quotation marks omitted). However, “Rule 9(b) requires only that the circumstances of fraud be stated with particularity; other facts may be pleaded generally, or in accordance with Rule 8.” *United States ex rel. Lee v. Corinthian Colls.*, 655 F.3d 984, 992 (9th Cir. 2011). In deciding a motion to dismiss for failure to state a claim, the court accepts all of the factual allegations as true and draws all reasonable inferences in favor of the plaintiff. *Usher v. City of Los Angeles*, 828

F.2d 556, 561 (9th Cir. 1987). But the court is not required to accept as true “allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

## II. MOTION TO STRIKE

Federal Rule of Civil Procedure 12(f) authorizes a court to “strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter.” Fed. R. Civ. P. 12(f). The function of a motion to strike “is to avoid the expenditure of time and money that must arise from litigating spurious issues by dispensing with those issues prior to trial.” *Sidney–Vinstein v. A.H. Robins Co.*, 697 F.2d 880, 885 (9th Cir.1983). Motions to strike are generally disfavored and “should not be granted unless the matter to be stricken clearly could have no possible bearing on the subject of the litigation.” *Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1057 (N.D. Cal. 2004). In addition, courts often require some showing of prejudice by the moving party before granting a motion to strike. *Hernandez v. Dutch Goose, Inc.*, No. C 13- 03537 LB, 2013 WL 5781476, at \*5 (N.D. Cal. Oct. 25, 2013).

“If the court is in doubt as to whether the challenged matter may raise an issue of fact or law, the motion to strike should be denied, leaving an assessment of the sufficiency of the allegations for adjudication on the merits.” *Carolina Cas. Ins. Co. v. Oahu Air Conditioning Serv., Inc.*, 994 F. Supp. 2d 1082, 1090-91 (E.D. Cal. 2014). In resolving a motion to strike, the pleadings must be viewed in the light most favorable to the nonmoving party. *Platte Anchor Bolt*, 352 F. Supp. 2d at 1057.

## III. MOTION TO DISMISS FOR LACK OF PERSONAL JURISDICTION

Where a defendant seeks dismissal for lack of personal jurisdiction, the plaintiff has the burden to demonstrate that personal jurisdiction exists. *In re W. States Wholesale Natural Gas Antitrust Litig.*, 715 F.3d 716, 741 (9th Cir. 2013). “However, the plaintiff must make only a prima facie showing of jurisdictional facts to withstand the motion to dismiss.” *Id.* (internal quotation marks omitted). “[U]ncontroverted allegations in the complaint must be taken as true,” and “[c]onflicts between parties over statements contained in affidavits must be resolved in the plaintiff’s favor.” *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir.

2004) (internal quotation marks omitted). But the court “may not assume the truth of allegations in a pleading which are contradicted by affidavit.” *Data Disc, Inc. v. Sys. Tech. Associates, Inc.*, 557 F.2d 1280, 1284 (9th Cir. 1977).

## DISCUSSION

### I. UBIQUITI MOTION TO DISMISS

#### A. Digital Millennium Copyright Act Claims

Synopsys alleges that defendants violated three provisions of the Digital Millennium Copyright Act. Ubiquiti and Tsai (collectively, Ubiquiti) move to dismiss the claims asserted under 17 U.S.C. § 1201(a)(2) and § 1201(b).<sup>4</sup>

##### 1. Sufficiency of Trafficked Allegations

As explained by the Ninth Circuit, section 1201(a)(2) “prohibits trafficking in technology that circumvents a technological measure that ‘effectively controls access’ to a copyrighted work” and (b) “prohibits trafficking in technology that circumvents a technological measure that ‘effectively protects’ a copyright owner’s right.” *MDY Indus., LLC v. Blizzard Entm’t, Inc.*, 629 F.3d 928, 942 (9th Cir. 2010), as amended. Together, 17 U.S.C. section 1201(a)(2) and section 1201(b) prohibit the “manufacture, import, offer to the public, provide, or otherwise traffic” in any technology that “is primarily designed or produced for the purpose of circumventing” technology or other protections of copyrighted works. Ubiquiti argues that Synopsys fails to specify what acts it allegedly took (manufacture, import, provide, or traffic) and fails to allege sufficient facts showing how those acts occurred, *e.g.*, what specific actions each defendant took to either manufacture, import, provide, or traffic in unauthorized license keys. Ubiquiti also argues that mere use of keys made by third-parties cannot constitute “manufacture, trafficking, or providing keys” because “mere use” does not violate Sections 1201(a)(2) or (b). And as to “provide,” Ubiquiti contends there must be allegations that defendants provided the circumvention technology to third-parties. Ubiquiti MTD at 5.

---

<sup>4</sup> Ubiquiti does not move to dismiss the circumvention claim prohibiting use of counterfeit and illicit license keys to circumvent restricted access to copyrighted materials under 17 U.S.C. § 1201(a)(1).

1 In Opposition, Synopsys points to allegations that all three defendants:

- 2 • “manufactured” circumvention technology creating counterfeit license keys, AC ¶¶ 28, 33,  
3 51, 57, 58;
- 4 • “imported” circumvention technology by transmitting circumvention technology from  
5 Taiwan to the United States, AC ¶¶ 42, 56, 58, 59, 66, 80;
- 6 • “provided” circumvention technology to one another over shared networks for commercial  
7 purposes, AC ¶¶ 60-63;
- 8 • and “otherwise trafficked” in circumvention technology by distributing the technology  
9 from Ubiquiti to UNIL and back in furtherance of their commercial objectives, AC ¶¶ 8, 9,  
10 12.

11 As to mere use, Synopsys notes that it alleges that defendants have been “secretly using  
12 counterfeit keys obtained and/or *created* with tools obtained through hacker websites to  
13 circumvent Synopsys’ License Key system” and access and use Synopsys’ EDA. AC ¶ 28  
14 (emphasis added). The and/or clause gets Synopsys beyond mere use. *See also id.* ¶ 57 (“The  
15 volume and nature of counterfeit keys used by the Piracy Enterprise, . . . indicate that one or more  
16 persons acting on behalf of the Piracy Enterprise used counterfeit key generation software to  
17 create counterfeit Synopsys license keys for use by Ubiquiti and UNIL.”).

18 Synopsys argues and I agree that with respect to manufacture and import, there is no need  
19 to show that the circumvention technology was made available to any third-parties; the unilateral  
20 actions of Ubiquiti in manufacturing the keys using software secured from hacker websites (not, as  
21 Ubiquiti alleges, merely using keys secured from those sites, AC ¶¶ 28, 57) and importing those  
22 keys from Taiwan into the United States is sufficient. AC ¶ 58.

23 As to importation, in its Reply Ubiquiti argues that “importation” is not sufficiently alleged  
24 and that allegations that the keys were “distributed” between the defendants is insufficient. In  
25 absence of apposite case law, I disagree. The plausible inference – given the locations of these  
26 separate corporate entities – is that importation from Taiwan to California occurred. Ubiquiti also  
27 challenges whether “remote access” to keys can satisfy the importation prong, but given that  
28 Synopsys has alleged that counterfeit keys were run on computers (or servers) *based* in California,

the access is not always “remote.” The allegations are sufficient.

As to manufacture, in Reply Ubiquiti argues that “human readable alphanumeric text elements” like the keys at issue are not items that are “manufactured.” Ubiquiti cites no case law in support of this novel argument, an argument that would seem to cut a wide swath away from the protections ensured by the *Digital Millennium Copyright Act*. Ubiquiti also relies on *Ass’n for Info. Media & Equip. v. Regents of the Univ. of California*, No. CV 10-9378 CBM MANX, 2011 WL 7447148 (C.D. Cal. Oct. 3, 2011) to argue that Synopsys’ manufacture allegations are insufficient. Ubiquiti MTD 5. But in that case, the complaint alleged only that defendants “worked with” another entity to “make circumvention applications available for higher education” but did not disclose “how the Defendants worked with Video Furnace, or what actions Defendants took that constitute the ‘manufacture, import, offer to the public, prov[ision], or otherwise traffic[king]’ of the DVDs.” *Id.* \*7. Here, the AC explains the relationship between the parties and that given the “volume and nature” of the keys, one or more persons “used counterfeit key generation software” to create the keys, distributed amongst themselves the keys and/or software. AC ¶¶ 57-58. That is sufficient.

With respect to “provide,” the allegations that defendant UNIL provided the circumvention technology to the separate corporate entity Ubiquiti is sufficient. In support, Ubiquiti relies on a different decision in the *Ass’n for Info. Media & Equip. v. Regents of the Univ. of California* case. There the defendants – the University and named administrators and employees – allegedly provided the at-issue software to its professors, but the Court concluded that because under the DCMA “these professors are not members of the public,” plaintiffs failed to state a claim. *Ass’n for Info. Media & Equip.*, 2012 WL 7683452, at \*9 (C.D. Cal. Nov. 20, 2012). That case is starkly different in that these separate corporate entities who – as addressed below – defendants argue must be treated differently for purposes of establishing jurisdiction, have provided the keys and/or key-creating-software to each other.<sup>5</sup>

---

<sup>5</sup> Relatedly, Ubiquiti argues that there must be allegations that the circumvention technology is being “offered” to third-parties. However, that language seems to have arisen in more typical DMCA cases where the defendant is an entity offering the circumvention technology to third-parties. Ubiquiti MTD at 5-6. Each of Ubiquiti’s cases simply quote *Chamberlain Grp., Inc. v.*

Finally, “trafficking” will be addressed below under 18 U.S.C. § 2318, as both sides agree the definition of trafficking there should be synonymous with trafficking under the DMCA.

## 2. Allegations that License Keys Prevent Infringement

Ubiquiti argues that because Section 1201(b) prevents circumvention of technological measures that are in place to protect a copyright owner, to state a claim under this section Synopsys must allege that its anti-circumvention technology prevents infringement – meaning prevents copying. Ubiquiti contends that Synopsys’ AC fails to allege prevention of infringement because the allegations are that Synopsys’ license keys merely control access to Synopsys’ EDA software and ensure that only a limited number of licensed users access it. Ubiquiti MTD at 5. In Opposition, Synopsys notes that when software is run on a machine a “copy” is made in the computer’s random access memory (RAM), and that copying (if without permission of the owner) constitutes copyright infringement. *See, e.g., MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 (9th Cir. 1993). By preventing its EDA software from executing on a machine without a valid key, Synopsys contends the key system prevents that sort of RAM copying and, therefore, prevents infringement. *Id.* These allegations are sufficient.

Synopsys has adequately alleged that defendants manufactured, imported, and provided circumvention devices in violation of Sections 1201(a)(2) and (b).

### B. 18 U.S.C. § 2318

18 U.S.C. § 2318, the Anti-Counterfeiting Act, prohibits the trafficking of counterfeit and illicit “labels,” including “labelling components” used by copyright owners to identify copies or computer programs and to verify that copies are not counterfeit or infringing. Under the statute, a “counterfeit label” is an identifying label that appears to be genuine, but is not. 18 U.S.C. §

---

*Skylink Techs., Inc.*, 381 F.3d 1178, 1203 (Fed. Cir. 2004) (claims under (a)(2) require showing “(1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) *that third parties can now access* (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.”) (emphasis added). At this juncture, I will let this claim go forward. However, as the discovery develops, Ubiquiti and UNIL may argue this issue again on summary judgment.

2318(b)(1). An “illicit label” is a genuine article “misused” in violation of the statute. *See, e.g., Microsoft Corp. v. Pronet Cyber Techs., Inc.*, 593 F. Supp. 2d 876, 878 (E.D. Va. 2009).

Synopsys argues that defendants are liable for trafficking in both counterfeit labels (counterfeit license keys) and illicit labels (valid but misused temporary license keys).

# 1. **Trafficked**

Trafficked, as defined by the statute means: “to transport, transfer, or otherwise dispose of, to another, for purposes of *commercial advantage* or private *financial gain*, or to make, import, export, obtain control of, or possess, with intent to so transport, transfer, or otherwise dispose of.” 18 U.S.C. § 2320(f)(5) (emphasis added). The term “financial gain” includes the receipt, or expected receipt, of anything of value. *Id.* § 2320(f)(2).

Ubiquiti argues that under the plain meaning of trafficked, Synopsys fails to state a claim because the only allegation is that defendants distributed or shared keys between themselves and there are no allegations that the license keys were offered to others or for purposes of commercial gain. In Opposition, Synopsys responds that its allegations that defendants “transferred” the keys to each other for their commercial gain – use of the software without paying license fees – is sufficient.<sup>6</sup> Synopsys argues that there is no need to allege the keys were “offered to others” as cases have recognized that producing infringing items or shipping illicit labels violate the act even where sales to others did not occur. *See, e.g., United States v. Beydoun*, 469 F.3d 102, 105 (5th Cir. 2006) (“even if Beydoun never sold a single infringing booklet, he remains accountable for the full amount, as he admits he caused infringing items to be produced with the intent to sell them”); *Microsoft Corp. v. Ion Techs. Corp.*, 484 F. Supp. 2d 955, 961 (D. Minn. 2007) (simply shipping illicit labels was sufficient to constitute a violation of the Act).

However, the cases relied on by Synopsys contemplate or expressly recognize that the defendants found liable under § 2318 at least had the *intent* to sell or transfer the illicit goods to

---

<sup>6</sup> In Reply, Ubiquiti argues that there are no allegations that defendants exchanged the keys for “commercial advantage,” *i.e.*, in commerce or trade, but simply for mere use. However, there is an obvious commercial advantage to using counterfeit keys in lieu of purchasing licenses and the use of those keys, as transferred from UNIL to Ubiquiti without purchase of a license by UNIL, and from Ubiquiti to UNIL without purchase of a license by Ubiquiti, was to their commercial advantage.



others, even if those sales or distributions were not actualized. *See, e.g., Beydoun*, 469 F.3d at 105. Nonetheless, Synopsys argues that it has stated this claim because it has alleged that defendants intended to transfer the illicit keys *to each other* for their commercial gain. Synopsys contends that the Ninth Circuit has affirmed a conviction based on similar sales between co-conspirators. *Oppo*. at 8 (relying on *United States v. Bao*, 189 F.3d 860, 863 (9th Cir. 1999)). But in *Bao*, the co-conspirators were convicted of conspiracy to violate Section 2138 where each printed part of illicit Microsoft products, all of which were obviously intended for sale to others outside of the conspiracy.

This is a close call. The cases cited by both sides simply demonstrate that the statute’s focus (or at least past application) is on conduct where a defendant or defendants produce or secure counterfeit or illicit labels that are logically intended for other non-defendant end users (DVDs, software COAs, etc.). Synopsys cites no cases showing that the statute’s definition of trafficking extends to a conspiracy where the labels were exchanged *only* to aid another defendant’s use of a copyrighted product. However, Ubiquiti cites no cases *excluding* from the reach of trafficking cases where the only intended recipient of the illegal labels was a co-conspirator/related defendant.<sup>7</sup> As such, I will not – as this juncture and based on briefing to date – dismiss this claim for failure to plead trafficking.

## 2. Counterfeit Labels

Ubiquiti argues that the fake keys allegedly created or used by defendants cannot be “counterfeit labels” because they are not “identifying labels” for Synopsys’ computer programs. Instead, because the fake keys were distributed apart from Synopsys software programs and the keys – standing on their own – do not identify anything about Synopsys’ EDA programs, they cannot be labels as they do not serve the “identifying” purpose of the statute. Ubiquiti MTD at 7-8. Synopsys responds by noting that the statute allows the labels to “accompany” the software, which is what occurred here albeit by separate email. It also cites a number of cases that have

---

<sup>7</sup> As added support, Ubiquiti cites legislative history noting that “trafficking” excludes those who knowingly acquire counterfeit articles solely for “personal use.” Ubiquiti MTD at 7, n.2. The allegations here, however, are that the defendants who are separate entities exchanged the labels for each of their commercial gain.

1 recognized that computer software access “keys” qualify as “identifying labels” under Section  
2 2318. Ubiquiti distinguishes those cases by noting that all of them address “keys” that were  
3 physically provided to customers when they purchased physical versions of software (*e.g.*, DVDs)  
4 or were otherwise attached to certificate of authenticity (COA) labels for the software products.  
5 Ubiquiti contends that no case has concluded that mere “electronic keys” without more are  
6 identifying labels under Section 2318. Ubiquiti MTD 8; Reply 4-5.<sup>8</sup>

7 At oral argument, Synopsys argued that evidence will show that when the keys were  
8 transmitted, they were accompanied by Synopsys logos and/or other information and indicia that  
9 served the “identifying” aspect of the statute. Those allegations, however, are not in the AC.  
10 Absent allegations showing how the keys, and the information transmitted with them, could fulfill  
11 the “identification” purpose of the statute, there is no basis to stretch Section 2318 to cover the  
12 distribution of the keys without any context *associating* them as Synopsys labels.<sup>9</sup>

---

13  
14 <sup>8</sup> See, *e.g.*, *United States v. Harrison*, 534 F.3d 1371, 1372 (11th Cir. 2008) (defendant convicted  
15 under 18 U.S.C. § 2318 of selling “stand-alone” COAs containing keys that could be used to  
16 activate a Microsoft program); *Microsoft Corp. v. Buy More, Inc.*, 136 F. Supp. 3d 1148, 1153  
17 (C.D. Cal. 2015) (granting summary judgment to plaintiff where “Product Keys obtained by one  
18 Defendant through the RRP website were wrongfully added to illicit and adulterated RRP COAs  
19 distributed by other Defendants”); *Microsoft Corp. v. Pronet Cyber Techs., Inc.*, 593 F. Supp. 2d  
20 876, 879 (E.D. Va. 2009) (“Defendants aver that they did not know any Product Keys printed on  
21 labels affixed to the products they sent were counterfeit or unauthorized.”); *Microsoft Corp. v.*  
22 *EEE Bus. Inc.*, 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008) (“By distributing a VLK without  
23 authorization, Wang effectively circumvented Microsoft’s technological measure to control access  
24 to a copyrighted work in violation of the DCMA. . . . Additionally, the VLK’s placement on a  
25 counterfeit label which accompanied the Volume License versions of the Windows XP and Office  
26 2003 software that Wang sold to Microsoft’s investigators constitutes trafficking in counterfeit  
27 labels.”); *Microsoft Corp. v. Silver Star Micro, Inc.*, No. 1:06-cv-1350-WSD, 2008 U.S. Dist.  
28 LEXIS 1526, at \*5 (N.D. Ga. Jan. 9, 2008) (“counterfeit product key label and product key”  
sold); *Microsoft Corp. v. Ion Techs. Corp.*, 484 F. Supp. 2d 955, 961 (D. Minn. 2007) (stand-alone  
COAs shipped); *Microsoft Corp. v. A Plus Open LLC*, No. 05-cv-00700-RPM, 2007 U.S. Dist.  
LEXIS 8435, at \*1 (D. Colo. Feb. 6, 2007) (distribution of “Microsoft Certificates of Authenticity  
without the corresponding Microsoft software program”); *Microsoft Corp. v. Sellers*, 411 F. Supp.  
2d 913, 917 (E.D. Tenn. 2006) (noting that “[a]n illicit COA is a genuine COA that is distributed  
or intended for distribution without the copy of software that Microsoft meant for it to accompany,  
including stand-alone COAs at issue here.”); *Microsoft Corp. v. # 9 Software, Inc.*, No. 4:05cv106,  
2005 U.S. Dist. LEXIS 36710, at \*2-3 (E.D. Va. Dec. 15, 2005) (“Defendants distributed  
Certificates of Authenticity without the Windows 2000 Pro and Windows XP software packages  
that Plaintiff intended the Certificates of Authenticity to accompany.”).

<sup>9</sup> To be clear, I agree with Synopsys that the keys do not have to physically accompany the  
software product to be considered labels, but they have to be delivered along with something  
suggesting the keys are being delivered in connection with a specific software product to be an  
“identifying label.”

Even if the keys could be counterfeit labels, Ubiquiti alleges that Synopsys fails to satisfy the gist of the statute (that the keys “appeared to be genuine” when the employees of the defendants who shared them allegedly knew they were not). Synopsys argues that this element is unnecessary; pointing to many cases where defendants were liable for trafficking even though their role was only a sale to another buyer who knew the products were not genuine. *Oppo*. 9. Synopsys misses Ubiquiti’s point; the aim of the statute is to prevent “false representations” and passing off of counterfeit material as real, of which there is no evidence here.

Recognizing the problems with the existing allegations, Synopsys offers to amend to allege the following:

that (1) Synopsys sent to Tsai a single delivery email containing links to download VCS and a license key for VCS; (2) Synopsys’ license keys are comprised of human readable alphanumeric text elements that identify which version and features of Synopsys products have been licensed for use in connection with a particular user’s copy of software; and (3) that the counterfeit keys used by Defendants mimicked the human readable text and format of Synopsys’ genuine keys, including text indicating that Synopsys is the “issuer” of the keys, and would thus appear to an innocent reader of the key file to be a genuine Synopsys license key.”

*Oppo*. 9-10 n.8. This amendment would bring the license keys closer to “identifying labels.” It would not, however, address the lack of facts supporting an allegation that Ubiquiti and UNIL intended to sell or trade or otherwise “pass off” the keys to an unsuspecting user. At this juncture and as with the Ubiquiti’s argument on “trafficking,” I am not convinced of its “gist of the statute” argument.<sup>10</sup>

Therefore, Synopsys is given leave to amend to add facts regarding how the keys served the identifying purpose of the statute. If Synopsys is able to plead those additional facts, Ubiquiti may re-raise its “gist of the statute” argument on a subsequent motion to dismiss providing more

---

<sup>10</sup> Synopsys points out that under a related section of the statute, 18 U.S.C. § 2320 (“Trafficking in counterfeit goods or services”), sellers “of imitation items ha[ve] violated trademark law if disinterested members of the general public would be confused were they to encounter the goods after sale. A seller can be convicted even though the direct buyer knows the goods are knock-offs.” *Wang v. Rodriguez*, 830 F.3d 958, 962 (9th Cir. 2016) (collecting cases). Those trademark cases, however, still expressly consider whether a theoretical “innocent” third-party buyer would be misled.

case law or legislative history support.

### 3. Illicit Labels

Under Section 2318, “illicit labels” are defined as “a genuine certificate, licensing document, registration card, or similar labeling component” that is used by an owner to “verify” that a copy of a computer program is not counterfeit or infringing, that is used without the authorization of the copyright owner, as follows:

- (i) distributed or intended for distribution not in connection with the copy [] to which such labeling component was intended to be affixed by the respective copyright owner; or
- (ii) in connection with a genuine certificate or licensing document, knowingly falsified in order to designate a higher number of licensed users or copies than authorized by the copyright owner, unless that certificate or document is used by the copyright owner solely for the purpose of monitoring or tracking the copyright owner’s distribution channel and not for the purpose of verifying that a copy [] is noninfringing.

18 U.S.C. § 2318(b)(4).

Ubiquiti argues that the keys cannot be “illicit labels” because their only purpose is to help Synopsys control its distribution channel and not (as required by the statute) to help Synopsys *identify* that someone is using a counterfeit or infringing copy of its EDA software. Ubiquiti MTD at 8-9. While Synopsys is correct that the AC alleges that the keys prevent “execution” of the software, AC ¶ 26, there is no explanation of how the genuine keys enable Synopsys to *verify* whether a particular copy of its software installed on a user’s system is counterfeit or infringing, or being used without their permission. Its reliance on *Microsoft Corp. v. Pronet Cyber Techs., Inc.*, 593 F. Supp. 2d 876 (E.D. Va. 2009) is misplaced. There the facts were that plaintiffs maintained “an internal list that matches each copy of a particular program to that copy’s unique Product Key.” *Id.* at 878. There are no facts alleged here to show how each genuine Synopsys license key is matched to a *particular copy* of a Synopsys EDA program, or that the genuine keys otherwise help Synopsys verify or monitor who is using its EDA programs.

Second, Ubiquiti argues that Synopsys fails to plead that the legitimate license keys were distributed by Ubiquiti or UNIL “not in connection” with the evaluation copies Ubiquiti or UNIL were permitted (at the relevant times) to use. Ubiquiti MTD 9. Synopsys responds that it has

adequately pleaded that the legitimate keys were used with unauthorized copies of its software. Oppo. 10 (citing AC ¶¶ 37, 39, 51, 59). However, the paragraphs of the AC Synopsys cites do not allege that defendants “made *unauthorized* copies of Synopsys’ software and then improperly used *someone else’s* legitimate temporary key to access those unauthorized copies.” Oppo. 10 (emphasis in original).

In light of these deficiencies, the claims regarding both counterfeit and illicit labels are DISMISSED with leave to amend.

### C. Civil RICO

The RICO statute, 18 U.S.C. § 1962(c) requires a plaintiff to prove that each defendant participated: in (1) the conduct of (2) an enterprise that affects interstate commerce (3) through a pattern (4) of racketeering activity, which (5) the proximately harmed the victim. *See Eclectic Properties E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 997 (9th Cir. 2014). To show an enterprise, “plaintiffs must plead that the enterprise has (A) a common purpose, (B) a structure or organization, and (C) longevity necessary to accomplish the purpose.” *Id.* “Racketeering activity,” as defined in 18 U.S.C. § 1961(1)(B), is the commission of a predicate act that is one of an enumerated list of federal crimes, which in this case are alleged to be: (i) violation of 18 U.S.C. § 2318, the Anti-Counterfeiting Act; (ii) fraud in connection with “access devices” under 18 U.S.C. § 1029; (iii) criminal copyright infringement under 17 U.S.C. § 506; and (iv) wire fraud under 18 U.S.C. § 1343.

Ubiquiti argues that Synopsys has failed to allege both a predicate act and the existence of an enterprise that engaged in a pattern of racketeering activity.<sup>11</sup>

#### 1. Predicate Act

##### a. Anti-Counterfeiting Act

As noted above, Synopsys has failed to alleged a claim under 18 U.S.C. § 2318. That claim cannot, for purposes of this motion, satisfy the predicate act requirement.

---

<sup>11</sup> Ubiquiti argues in passing that the AC does not identify Ubiquiti and UNIL as members of the Piracy Enterprise. When read fairly, the AC identifies them as members. *See, e.g.*, AC ¶¶ 29, 31, 126, 127.

**b. Access Device Fraud Under 18 U.S.C. § 1029**

18 U.S.C. § 1029 criminalizes the production, use, or trafficking in “counterfeit access devices” with intent to defraud. The statute defines access devices as:

any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

Section 1029(e)(1). Ubiquiti argues that the statute is primarily directed to credit card and banking system frauds, and asserts that the conduct alleged here is starkly different. As a result, Ubiquiti contends that Synopsys has not alleged, and is unable to allege, facts showing that the license keys can be considered access devices that are used to access a Synopsys “account” as required by the statute. There needs to be, but are not, allegations about improper access to an account in Synopsys’ EDA software delivery and access system.

I agree that the conduct alleged here does not fit neatly within the apparent purpose and aim of the statute, even if broadly construed,<sup>12</sup> but nothing in the language of the statute excludes its application to this type of case and no cases cited by Ubiquiti have declined to apply it in light of similar allegations. Ubiquiti, however, is correct that Synopsys has failed to allege sufficient facts describing the actual or functional “account”<sup>13</sup> Ubiquiti allegedly accessed using the counterfeit access device and that Ubiquiti accessed the account in order to “obtain money, goods, services, or any other thing of value” as required. Therefore, this predicate act is DISMISSED with leave to amend.

**c. Criminal Copyright Infringement Under 17 U.S.C. § 506**

Under 17 U.S.C. § 506, criminal copyright infringement occurs when a person “willfully

---

<sup>12</sup> See, e.g., *United States v. Bailey*, 41 F.3d 413, 417 (9th Cir. 1994) (“[T]he purpose of the statute is to deal with the abuse of new technologies that increasingly allow individuals and businesses access to goods and services without immediate payment by cash or familiar, paper instruments.”)

<sup>13</sup> “[A]n account is a contractual relationship that makes possible the provision of goods, services, or money based on payment, or the expectation of payment, at some later point in time, as described by the entry of credits and debits in a formal record.” *Bailey*, 41 F.3d at 417.

1 infringes a copyright” if the infringement was committed “(A) for purposes of commercial  
2 advantage or private financial gain; (B) by the reproduction or distribution, including by electronic  
3 means, during any 180-day period, of 1 or more copies [] of 1 or more copyrighted works, which  
4 have a total retail value of more than \$1,000.”

5 Ubiquiti argues that “run-of-the-mill” copyright infringement cases such as this one cannot  
6 be a RICO predicate act because of the legislative history showing that Congress’s concern was  
7 with piracy and counterfeiting when it added criminal copyright as a RICO predicate act. Ubiquiti  
8 MTD at 13-14; *Stewart v. Wachowski*, No. CV 03-2873 MMM VBKX, 2005 WL 6184235, at \*6  
9 (C.D. Cal. June 14, 2005) (“The court can find no legislative history consistent with a  
10 Congressional intent to expand RICO liability to all knowing copyright infringement, including  
11 acts that cannot be characterized as counterfeiting or piracy”); 5 Nimmer on Copyright § 15.05  
12 (2017) (“Only the most egregious instances of criminal copyright infringement have ever been  
13 upheld as predicate offenses to racketeering charges under RICO.”); *see also Robert Kubicek*  
14 *Architects & Assocs. Inc. v. Bosley*, No. CV 11-2112 PHX DGC, 2012 WL 3149348, at \*2 (D.  
15 Ariz. Aug. 1, 2012) (rejecting as RICO predicate act allegation of copyright infringement where  
16 defendants were accused of using plaintiff’s copyrighted architectural drawings because there was  
17 no suggestion of “piracy or counterfeiting”)

18 In opposition, Synopsys relies on cases that have rejected the *Stewart* court’s reliance on  
19 legislative history (showing a particular concern over piracy and counterfeiting enterprises), and  
20 instead applied the “plain language” of RICO which requires only “any” act of criminal copyright  
21 infringement, no matter its size or impact. *See, e.g., ICONICS, Inc. v. Massaro*, 192 F. Supp. 3d  
22 254, 269 (D. Mass. 2016) (permitting allegations of copyright infringement stemming from a  
23 business dispute between two companies to be a predicate act under RICO). Synopsys also asserts  
24 that while the alleged infringement might have been “small-scale” in terms of those involved (just  
25 the three defendants), its allegations are of sufficient significance that this claim should be allowed  
26 to proceed. At this juncture, I agree. Synopsys alleges a scheme of copyright infringement that  
27 allowed defendants to avoid paying millions in license fees for multiple EDA programs that  
28 extended for a period of years. That is sufficient for criminal copyright as a predicate act.

Ubiquiti also argues that Synopsys has failed to allege sufficient facts that: (i) Synopsys owns copyright rights; (ii) defendants violated some portion of Synopsys’ exclusive rights under 17 U.S.C. § 106;<sup>14</sup> and (iii) defendants’ acts were willful. I disagree. Synopsys has alleged that it owns copyrights in the software at issue (AC ¶ 24); that defendants made, distributed, and used copies without authorization in order to avoid paying license fees and benefit from that software (AC ¶¶ 28, 29, 42, 45, 56, 63, 65); and that those acts were willful. AC ¶¶ 43, 65. As to the allegations that defendants intended to exceed the scope of their temporary evaluation license, that is also adequately alleged. AC ¶¶ 41, 42, 56.

Synopsys’ allegations, especially when considered in the context of the scheme alleged, are sufficient to allege criminal copyright infringement.

**d. Wire Fraud Under 18 U.S.C. § 1343**

To prove wire fraud, plaintiff must show: (i) the formation of a scheme to defraud, (ii) the use of interstate wires in furtherance of that scheme, and (iii) the specific intent to defraud. *Eclectic Properties E., LLC*, 751 F.3d at 997.

Ubiquiti argues first that Synopsys fails to allege use of interstate wires to facilitate the fraud because neither of the two wire transmissions identified in the AC – emails from Tsai to Synopsys on October 14, 2013 (AC ¶ 38) and emails from Tsai to Synopsys on December 2, 2013 (AC ¶ 46) – were fraudulent in and of themselves. But as Synopsys points out, the emails themselves do not need to be stand-alone actionable frauds as long as they were in furtherance of the fraudulent scheme.<sup>15</sup> Synopsys also points to other wire transmissions – although not individually identified in the RICO “wire fraud” section of the AC – that were used in furtherance

---

<sup>14</sup> Defendants argue that Synopsys does not identify the specific software it believes defendants copied and distributed, or that defendants copied and distributed those specific titles (as opposed to mere use). Ubiquiti MTD Reply 9. But Synopsys adequately alleges unauthorized “access and use” of identified titles (*see, e.g.*, ¶ 28), as well as the making and distributing copies of that software (AC ¶ 29). Moreover, as noted above, “copying” occurs when a software program is “used” to the extent it is loaded into a computer’s RAM. These allegations are sufficient.

<sup>15</sup> *See, e.g., United States v. Lo*, 231 F.3d 471, 478 (9th Cir. 2000) (discussing analogous mail fraud statute and noting that while “a mailing must occur in the execution of the scheme . . . the mailing need not be an essential element of the scheme. Rather, it is sufficient if the mailing is ‘incident to an essential part of the scheme’”).



of defendants' scheme to defraud, such as defendants' fraudulent access of Synopsys' servers in California over the internet and Tsai's and UNIL's continued contacts via email with Synopsys in California about Ubiquiti's and then UNIL's purported interests in evaluating the Synopsys software when those representations were part of the scheme to gain access to the software so it could be pirated.<sup>16</sup> The AC also sufficiently alleges that the defendants used the internet to send and access unauthorized copies of the software and the illegal keys.

Relatedly, Ubiquiti argues that Synopsys fails to identify with Rule 9(b) particularity: (i) what fraudulent representations or omissions were made to Synopsys; (ii) that they were false or misleading when made; (iii) that the misrepresentations and omitted facts were material; (iv) that Synopsys relied on them to its detriment; and, (v) with respect to omissions, that Tsai owed a duty to disclose to Synopsys. Ubiquiti MTD 17-18. However, the AC is replete with details regarding the fraudulent scheme; that Ubiquiti and UNIL, acting through Tsai, never intended to truly evaluate Synopsys' software but instead sought access in order to pirate it and that they did exactly that once they secured access through the evaluation license keys. How the scheme was carried out thereafter – with the creation of counterfeit license keys, repeated access of Synopsys' websites for documentation and support – is described in detail. The specific communications made by defendants to effectuate the scheme (emails and meetings) are repeatedly identified.<sup>17</sup>

Similarly, if the *only* allegations were that defendants accessed only the software programs allowed under the evaluation licenses, using only legitimate keys, installing the programs only on agreed-to computers, and accessing that software only during the timeframe agreed-to for evaluation, defendants' argument that Synopsys should be required to state *additional* facts showing why defendants' representations were false when made might carry some weight. But

---

<sup>16</sup> Ubiquiti argues that Synopsys has not alleged sufficient facts that the wires used were interstate, but the facts regarding UNIL's operation in Taiwan, the use of keys by UNIL employees, and computers associated with UNIL accessing and running Synopsys software through Synopsys' California-based servers are sufficient. Of course, if discovery does not demonstrate that interstate wires were used, this would be a ground for summary judgment.

<sup>17</sup> Ubiquiti's focus on cases addressing omissions and "failure to disclose" fraud theories that require pleading a statutory or fiduciary duty between the parties is misplaced. Ubiquiti MTD 17-18.

1 that is not this case as alleged. Allowing *this* case to go forward on a fraud theory will not turn  
2 every evaluation license negotiated between two parties when a license deal is not consummated  
3 into a potential fraud case. It is the additional conduct alleged here – the years-long impermissible  
4 access to Synopsys’ servers and use of their software thousands of times with counterfeit keys –  
5 that plausibly suggests fraudulent intent existed at the inception of the parties’ relationship.

6 Wire fraud has been adequately alleged as a predicate act.

7 **2. Pattern of Racketeering**

8 Ubiquiti also argues that a RICO “pattern” has not been alleged. However, Synopsys has  
9 alleged a scheme of first securing access to legitimate keys and software under fraudulent  
10 pretenses *and then* repeated and continued impermissible access to and use of that software over a  
11 period of three years using counterfeit keys. There is no support for defendants’ attempt to limit  
12 the scope of the racketeering activity to just the mere seven-month evaluation period. The fact  
13 that the fraud may have originally occurred towards the inception of the parties’ relationship  
14 (resulting in Ubiquiti and UNIL receiving temporary license keys) does not mean that the  
15 continued actions to effectuate the scheme (continued use of software with both legitimate and  
16 illegitimate keys created and shared by defendants, resulting in ongoing copyright infringement)  
17 are not part of the pattern.

18 Synopsys also argues it has alleged a sufficient threat of ongoing activity, contending that  
19 defendants still have Synopsys’ software on their systems and access to illegal keys. Defendants  
20 argue that these allegations are absent from the AC. Reply 13. Synopsys is given leave to include  
21 them in its Second Amended Complaint.

22 **3. Enterprise**

23 Under 18 U.S.C. § 1962(c), a plaintiff must prove the existence of at least two distinct  
24 entities: “(1) a ‘person’; and (2) an ‘enterprise’ that is not simply the same ‘person’ referred to by  
25 a different name.” *Cedric Kushner Promotions, Ltd. v. King*, 533 U.S. 158, 161 (2001). Synopsys  
26 has two theories of RICO enterprise. First, Ubiquiti and UNIL as otherwise legitimate businesses  
27 joined with Tsai and “other employees” to conduct the affairs of Ubiquiti and UNIL through a  
28 course of racketeering activity. Second, an association-in-fact enterprise (Piracy Enterprise) was

developed where Tsai, Ubiquiti, UNIL and others employees all came together to create the Piracy Enterprise and conduct the illegal acts.

Under section 1962(c), the “person” who allegedly violates the statute must be distinct from the “RICO enterprise” whose affairs that person is conducting or participating in. *Cedric Kushner Promotions, Ltd. v. King*, 533 U.S. 158, 162 (2001). Ubiquiti argues that Synopsys has not alleged a “person” distinct from the “RICO enterprise” because Ubiquiti and UNIL cannot be both RICO defendants/persons and the RICO enterprise, and the inclusion of Tsai, as a corporate employee of Ubiquiti, does not alter that fact. However, that Ubiquiti and UNIL are named as RICO defendants/persons does not necessarily mean that a distinct RICO enterprise cannot be alleged. The allegations are that Ubiquiti and UNIL, along with Tsai and other unidentified employees, came together for the purpose of conducting the affairs of Ubiquiti and UNIL through RICO-prohibited fraud and copyright infringement; these persons created an association in fact “Piracy Enterprise” that exists separately from the otherwise legitimate business of Ubiquiti and UNIL.

District courts in the Ninth Circuit are somewhat split on the question of what is required to show distinctness between related corporate entities. Some courts conclude that “the formal, legal separation of the defendant entities satisfies the RICO distinctiveness requirement.” *Waldrup v. Countrywide Fin. Corp.*, No. 2:13-CV-08833-CAS, 2015 WL 93363, at \*7 (C.D. Cal. Jan. 5, 2015); *see also Monterey Bay Military Hous., LLC v. Pinnacle Monterey LLC*, 116 F. Supp. 3d 1010, 1046 (N.D. Cal. 2015), *order vacated in part on reconsideration on other grounds*, No. 14-CV-03953-BLF, 2015 WL 4624678 (N.D. Cal. Aug. 3, 2015) (“Defendants cannot shed their other corporate distinctions when it suits them, particularly where it is alleged that the separate corporate entities were critical in carrying out the racketeering activity.”);<sup>18</sup> *Negrete v.*

---

<sup>18</sup> Judge Freeman in *Monterey Bay* distinguished the primary case relied on by Ubiquiti for the proposition that wholly-owned subsidiaries are not “distinct” enough to create an enterprise, *In Re Ice Cream Distributors of Evansville, LLC v. Dreyer's Grand Ice Cream, Inc.*, No. 09–5815 CW, 2010 WL 3619884 (N.D.Cal. Sept. 10, 2010), by noting that there was insufficient evidence in her case of whether the subsidiaries were wholly-owned and controlled by one defendant. 116 F. Supp. 3d. at 1046 n.20. The same is true here. Ubiquiti has been conspicuously vague – presumably in light of UNIL’s pending motion to dismiss for lack of jurisdiction – regarding the relationship between Ubiquiti and UNIL.

*Allianz Life Ins. Co. of N. Am.*, 926 F.Supp.2d 1143, 1151 (C.D.Cal.2013) (finding that the “formal separation [of parent and subsidiary companies] is alone sufficient to support a finding of distinctiveness”). Others require “something more” than mere legal distinctiveness, like different or uniquely significant role in the enterprise. *See, e.g., In re Countrywide Fin. Corp. Mortgage Mktg. & Sales Practices Litig.*, 601 F.Supp.2d 1201 (S.D.Cal.2009).

No matter which test I apply, at this juncture the allegations suffice to establish a RICO enterprise. The presence of a separate corporate entity – UNIL – takes this case a step away from cases finding insufficient distinctness where the alleged person is a corporate employee and the alleged enterprise is the corporation. Ubiquiti and UNIL are separate corporate entities alleged to have engaged in separate acts in furtherance of the conspiracy. This question may be revisited on summary judgment after discovery about the governance and operation of the two corporate entities is conducted and as more evidence comes to light regarding whether the association-in-fact enterprise was simply conducting its own affairs (*e.g.*, the affairs of the corporations) or the affairs of a distinct RICO enterprise.<sup>19</sup>

#### 4. No RICO Conspiracy Alleged

Finally, in addition to arguing that because Synopsys fails to allege a substantive RICO violation there can be no conspiracy, Ubiquiti argues that Synopsys’ conspiracy claim fails for the independent reason that Synopsys has failed to allege that any of the defendants “agreed to facilitate” the scheme; in other words that all three reached an agreement to conduct the RICO enterprise. All that the AC alleges, according to Ubiquiti, is that Tsai engaged in a series of actions, which is insufficient.

But in addition to the actions of Tsai, *other* employees of Ubiquiti and UNIL are alleged to have taken acts to support the conspiracy. Those allegations include the use of multiple illegal keys connected to the names of employees of Ubiquiti and UNIL other than Tsai, as well as the

---

<sup>19</sup> *See, e.g.,* Gregory P. Joseph, *Civil RICO a Definitive Guide 41* (ABA 2015) at § 9 (discussing “Distinctness and Association-in-Fact Enterprises” and cases that have found insufficient distinctness where the associated-in-fact enterprise is composed solely of the RICO defendant persons).

use at least 39,000 times of the counterfeit keys to circumvent the Synopsys' license key access-control, and where those keys were used on multiple computers and devices associated with Ubiquiti, UNIL, and others. AC ¶¶ 32, 59, 64. Fairly read, the allegations concern activities of all three, going far beyond the activities of Tsai. Given the scope of the alleged piracy here, agreement can be readily and plausibly inferred.

Therefore, Synopsys' RICO claim has been adequately pleaded and may proceed. Synopsys has leave to amend its Anti-Counterfeiting Act predicate acts (under 18 U.S.C. § 2318) and the Access Device Fraud predicate acts (under 18 U.S.C. § 1029).

#### **D. Fraud and Negligent Misrepresentation**

##### **1. Legal Standard**

Under FRCP 9(b), to state a claim for fraud, a party must plead with particularity the circumstances constituting the fraud, and the allegations must be specific enough to give defendants notice of the particular misconduct ... so that they can defend against the charge and not just deny that they have done anything wrong." *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir.2009) (citation omitted). "Averments of fraud must be accompanied by the who, what, when, where, and how of the misconduct charged." *Vess v. Ciba-Geigy Corp.*, 317 F.3d 1097, 1106 (9th Cir. 2003) (citation omitted).

##### **2. Adequacy of Allegations**

Ubiquiti generally reasserts the same arguments it made with respect to wire fraud as a predicate act in arguing that Synopsys fails to adequately allege fraud and negligent misrepresentation. However, Synopsys has identified the express representations made by Tsai that it believes were false when made (*i.e.*, that neither Ubiquiti nor UNIL had a honest and good faith intent to actually evaluate Synopsys' software and instead their intent was to copy and use it without a license) and why those representations were false when made (*i.e.*, the large scale pirating and deception that Ubiquiti and UNIL subsequently engaged in). Whether Synopsys will be able to prove these allegations is a different question, but Synopsys has adequately alleged the facts supporting these claims in its AC.

In sum, Ubiquiti's motion to dismiss is GRANTED in part. The claims under the Anti-

Counterfeiting Act (18 U.S.C. § 2318) are dismissed with leave to amend. The remaining claims may proceed, although Synopsys may amend the deficiently alleged predicate acts and threat of ongoing harm under its RICO claim.

## II. MOTION TO STRIKE AFFIRMATIVE DEFENSES

Ubiquiti’s declaratory relief counterclaim seeks a declaration that it cannot be liable for an act of circumvention under 17 U.S.C. § 1201. Its breach of contract counterclaim is based on Synopsys’ use of “monitoring software” placed in the software Synopsys provided to Ubiquiti and the subsequent transfer and use of Ubiquiti’s confidential information to third parties, which Ubiquiti claims violated the terms of the parties’ Master Non-Disclosure Agreement (MNDA). Ubiquiti moves to strike each of Synopsys’ affirmative defenses.

### A. Legal Standard

The parties disagree on whether the *Twombly/Iqbal* standard or the lower “fair notice” standard applies to determining whether affirmative defenses have been adequately pleaded. I previously agreed with my colleagues in this district that the *Twombly/Iqbal* standard applies to affirmative defenses. *See BlackBerry Ltd. v. Typo Prod. LLC*, No. 14-cv-00023-WHO, 2014 WL 1867009, at \*4-5 (N.D. Cal. May 8, 2014). However, the Ninth Circuit subsequently decided *Kohler v. Flava Enterprises, Inc.*, 779 F.3d 1016 (9th Cir. 2015). *Kohler* affirmed a district court’s finding that an affirmative defense was adequately pleaded, stating, “the ‘fair notice’ required by the pleading standards only requires describing the defense in ‘general terms.’” *Id.* at 1019. Since *Kohler*, many of my colleagues have nonetheless reaffirmed that *Twombly/Iqbal* apply to affirmative defenses. *See Murphy v. Trader Joe’s*, No. 16-CV-02222-SI, 2017 WL 235193, at \*2 (N.D. Cal. Jan. 19, 2017) (“*Kohler* did not directly address the pleading standard for affirmative defenses; the court touched on the issue only in passing. . . . Accordingly, in the absence of clear controlling authority, the Court will follow numerous decisions in this district applying the *Twombly/Iqbal* standard to affirmative defenses.”); *see also Prod. & Ventures Int’l v. Axis Stationary (Shanghai) Ltd.*, No. 16-CV-00669-YGR, 2017 WL 1330598, at \*3 (N.D. Cal. Apr. 11, 2017) (same); *Perez v. Wells Fargo & Company*, No. 14-cv-0989-PJH, 2015 WL 5567746, at \*3 (N.D. Cal. Sept. 21, 2015) (concluding *Kohler* “did not specifically hold . . . that

the *Twombly/Iqbal* standard does not apply to the pleading of affirmative defenses.”). Other courts, however, disagree. See *MyGo, LLC v. Mission Beach Indus., LLC*, No. 16-cv02350- GPC, 2017 WL 107346, at \*7 (S.D. Cal. Jan. 11, 2017) (applying “fair notice” standard); *Bcompany v. Courtesy Oldsmobile-Cadillac, Inc.*, No. 15-cv-01137, 2016 WL 615335, at \*3 (E.D. Cal. Feb. 16, 2016) (collecting cases applying fair notice standard).

Acknowledging that this issue is not settled, I will follow the most recent decisions from this Court and apply the *Twombly/Iqbal* standard. Under this standard, “a defense need not include extensive factual allegations,” but “bare statements reciting mere legal conclusions may not be sufficient.” *Perez v. Gordon & Wong Law Grp., P.C.*, No. 11-cv-03323-LHK, 2012 WL 1029425, at \*8 (N.D. Cal. Mar. 26, 2012). “In other words, the simple listing of ‘a series of conclusory statements asserting the existence of an affirmative defense without stating a reason why that affirmative defense might exist’ is not sufficient.” *Hernandez v. Dutch Goose, Inc.*, No. C 13-03537 LB, 2013 WL 5781476, at \*4 (N.D. Cal. Oct. 25, 2013).

## **B. Failure to State Sufficient Facts**

Ubiquiti moves to dismiss the following affirmative defenses as inadequately pleaded.

### **1. Waiver**

In its Waiver Affirmative Defense, Synopsys alleges:

Ubiquiti waived the rights, if any, underlying its counterclaims because Ubiquiti voluntarily and intentionally abandoned or relinquished such rights by expressly consenting to the complained of conduct in agreeing to Synopsys’ websites’ terms of use, which gave Ubiquiti notice of the complained of conduct (including that Synopsys would monitor login activity and access to its software) and required Ubiquiti to assent to such conduct. Ubiquiti also implicitly consented to Synopsys’ conduct in the course of communications with ITCA by confirming and sharing additional information with ITCA about Ubiquiti’s activities, employees, and purported proprietary information in or about the summer of 2016.

Amended Answer 7.

“Waiver is the intentional relinquishment of a known right with knowledge of its existence and the intent to relinquish it.” *Catch a Wave, Inc. v. Sirius XM Radio, Inc.*, No. C 12-05791 WHA, 2013 WL 1996134, at \*2 (N.D. Cal. May 13, 2013) (striking affirmative defense for waiver under *Twombly/Iqbal* standard for failure “to explain how or when plaintiff intentionally

relinquished any known right”).

Ubiquiti argues that Synopsys fails to adequately plead facts supporting waiver because it fails to allege: “(i) the language in the terms of use to which Ubiquiti allegedly assented, (ii) when the alleged assent occurred, (iii) where the alleged assent occurred (i.e., which website), and (iv) who allegedly assented on behalf of Ubiquiti.” Mot. to Strike 5. It contends that these failures are significant because of allegations Tsai makes in support of UNIL’s motion to dismiss for lack of personal jurisdiction as well as assertions Synopsys makes in opposition to that motion, which create ambiguities such that “Ubiquiti genuinely has no idea when or how it allegedly waived any rights, or what the scope of such a waiver might have been.” *Id.*, 5 n.2. However, any facts asserted or positions taken in response to the motion to dismiss for lack of personal jurisdiction are not properly subject to notice on a motion to dismiss or strike under Rule 12.

Ubiquiti also argues that because what *it* complains of is the improper “transmission, utilization, and disclosure” of Ubiquiti’s confidential information to third-parties in violation of the parties’ MNDA, its theoretical agreement allowing *Synopsys* to monitor log-in activity and access to its software cannot support waiver. Ubiquiti argues that the waiver defense is also “entirely conclusory” given the “vaguely” described terms of use that Synopsys contends Ubiquiti agreed to at an unidentified point in time.

I disagree. The applicable terms of use, when they were agreed to, and by whom, will be readily determined through discovery. What those terms of use expressly or reasonably allow will be determined at summary judgment or trial. Similarly, what the parties’ actual intent was with respect to the MNDA *versus* the terms of use will also be fleshed out during discovery and any legal issues will be resolved at summary judgment or trial. The facts alleged in support of this affirmative defense recite far more than “mere legal conclusions” and are sufficient as well as plausible. Ubiquiti – as shown in part by its merits-based arguments on Reply – knows exactly how to challenge this defense.<sup>20</sup>

---

<sup>20</sup> Ubiquiti makes a number of “merits” based challenges to the waiver argument regarding the subject matter of the MNDA; what it might have allowed or prohibited, and when it was entered into vis-à-vis the terms of use, but fails to attach the MNDA itself. In Opposition, Synopsys attaches both the MNDA and a version of its terms of use, arguing that those documents are



2. **Laches**

In its Laches Affirmative Defense, Synopsys alleges:

Ubiquiti’s counterclaims are barred by the doctrine of laches. Ubiquiti has known for years or at least many months of the complained of conduct (including that Synopsys would monitor login activity and access to its software) and failed to pursue any claim or raise any objection based on such conduct. Ubiquiti agreed to Synopsys’ websites’ terms of service in late 2013 and has known since that time of the complained of conduct. At the latest, Ubiquiti learned of Synopsys’ conduct in May 2016 when it received Synopsys’ cease and desist communications, yet Ubiquiti took no action. Synopsys will suffer evidentiary and economic prejudice as a result of Ubiquiti’s unreasonable delay.

Amended Answer 7.

To state a claim for laches, a defendant must allege that “(1) the plaintiff delayed in initiating the lawsuit; (2) the delay was unreasonable; and (3) the delay resulted in prejudice.” *Petrella v. Metro-Goldwyn-Mayer, Inc.*, 695 F.3d 946, 951–52 (9th Cir. 2012), *rev’d on other grounds* by 134 S. Ct. 1962 (2014). “Laches is an equitable defense that prevents a plaintiff, who ‘with full knowledge of the facts, acquiesces in a transaction and sleeps upon his rights.’” *Danjaq LLC v. Sony Corp.*, 263 F.3d 942, 950–51 (9th Cir. 2001) (internal citation omitted). As to prejudice, there are generally two kinds, evidentiary and expectations. “Evidentiary prejudice includes such things as lost, stale, or degraded evidence, or witnesses whose memories have faded or who have died. . . . A defendant may also demonstrate prejudice by showing that it took actions or suffered consequences that it would not have, had the plaintiff brought suit promptly.” *Id.* at 955 (internal citation omitted).

Related to its argument on waiver, Ubiquiti asserts that the terms of use did not give Synopsys the permission to engage in the conduct Ubiquiti complains of (the “transmission, utilization, and disclosure” of Ubiquiti’s confidential information to third-parties). Mere recitation to the terms of use in this affirmative defense is deficient, it contends, because it lacks factual

---

incorporated by reference by Ubiquiti’s counterclaim and by Synopsys’ Amended Answer. Exhibits A & C to Oppo. In Reply, Ubiquiti ignores the actual language of those documents and contends that they should be ignored because they are not supported by affidavit or declaration and are not authenticated. Reply 4 n.3. Both sides are making *merits* arguments that are not appropriately resolved here when the question is simply the adequacy of the pleading of the waiver affirmative defense.

1 allegations showing that Ubiquiti could have slept on its rights or had full knowledge of the facts  
2 from the alleged agreement to the terms of use in 2013. However, what was actually disclosed in  
3 the terms of use and what Ubiquiti or a reasonable company would have known or expected to  
4 have happened under those terms of use is something that will be determined after discovery and  
5 at summary judgment or trial.

6 Similarly, Ubiquiti complains that the cease and desist from Synopsys in 2016 could not  
7 have put Ubiquiti on notice that Synopsys had transmitted its confidential information to third  
8 parties. As above, what Ubiquiti or an objective company would have understood as to *how*  
9 Synopsys learned of Ubiquiti's alleged continued use of Synopsys' software in 2016 (and  
10 therefore whether Ubiquiti or a reasonable company should have known transmission of  
11 confidential data to a third party had occurred) as well as the exact contours of what was disclosed  
12 in that cease and desist will be fleshed out in discovery and determined through motion practice or  
13 at trial. For now, the facts alleged in support of this affirmative defense recite far more than "mere  
14 legal conclusions" and are sufficient as well as plausible.

15 As to the sufficiency of allegations of "prejudice" for laches, the type of prejudice claimed  
16 to have been suffered by Synopsys is not expressly pleaded but Synopsys is correct that given  
17 reasonable inference, the prejudice at issue is that relevant evidence has been lost since 2013 and  
18 that Synopsys' potential liability has increased over time. Oppo. 9.

### 19 3. Mitigation

20 In its Mitigation Affirmative Defense, Synopsys alleges:

21 Synopsys incorporates the factual allegations set forth above and the  
22 factual allegations of its Amended Complaint, including without  
23 limitation paragraphs 1 through 66. Ubiquiti has failed to mitigate or  
24 attempt to mitigate its damages, if any. Ubiquiti has known for years  
25 or at least many months of the complained of conduct (including  
26 that Synopsys would monitor login activity and access to its  
27 software), yet Ubiquiti undertook no effort to remedy the alleged  
28 unauthorized disclosure of its proprietary information.

Amended Answer 8. Ubiquiti moves to strike because (as above) it cannot be a defense to the  
complained-of conduct of disclosure of Ubiquiti's confidential information to third-parties because  
the terms of use address something else. I have already rejected that line of argument. As to the

point of *when* Ubiquiti discovered the wrong – and therefore when the duty to mitigate arose – that is subject to discovery (*e.g.*, when did or should Ubiquiti have understood given the terms of use that third-parties had access to its “confidential information” about IP addresses and users). Finally, Ubiquiti also moves to strike because “mitigation” is not really an affirmative defense but more of a factor in determining damages. However, because mitigation is relevant to and has a “plausible bearing” to this litigation (even if not a stand-alone affirmative defense), I will not strike it. *See Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1057 (N.D. Cal. 2004).

#### 4. Novation

In its Novation Affirmative Defense, Synopsys alleges:

Ubiquiti’s breach counterclaim is barred by the doctrine of novation. Subsequent to executing the contract underlying its counterclaim, on November 26, 2013, Ubiquiti consented in writing to a superseding Synopsys evaluation license agreement that expressly stated that it extinguished the obligations underlying Ubiquiti’s counterclaim and replaced them with new obligations under the evaluation license agreement.

Amended Answer 8.

“Novation is the substitution of a new obligation for an existing one.” Cal. Civ.Code, § 1530. “The substitution is by agreement and with the intent to extinguish the prior obligation.” *Wells Fargo Bank v. Bank of Am.*, 32 Cal. App. 4th 424, 431 (1995) (citing Cal. Civ.Code, §§ 1530, 1531). Under California law, a party attempting to prove “novation” must satisfy “four essential requisites”: (1) the existence of a previous valid obligation; (2) the agreement of all the parties to a new contract; (3) the extinguishment of the old contract; and (4) the validity of the new one. *See Miran v. Convergent Outsourcing, Inc.*, No. 316CV00692AJBJMA, 2017 WL 1410296, at \*3 (S.D. Cal. Apr. 20, 2017) (relying on *Young v. Benton*, 21 Cal. App. 382, 384 (1913)).

Ubiquiti initially argues that Synopsys fails to allege facts sufficient to establish novation because (i) Synopsys fails to adequately allege the contents of the superseding Synopsys evaluation license agreement and (ii) the subsequent evaluation license agreement could not novate the MNDA because those agreements govern distinct subject matters. Mot. to Strike 10-11. In Opposition, Synopsys attaches as exhibits the evaluation license and the MNDA; as noted above, Ubiquiti objects to my consideration of those documents and disputes their authenticity.

Reply 4 n.3. Nonetheless, apparently because Ubiquiti thinks consideration of the terms of those agreements is (for this argument) helpful to it, Ubiquiti addresses the contents of the MNDA and the evaluation license and argues that “[n]o rational objective reading of these agreements leads to the conclusion” that the evaluation license novated the MNDA. Reply 8 - 9. I will not get into the merits by comparing these two agreements or make findings as to when the agreements were entered into, because these arguments were raised only on reply. It is sufficient for present purposes that Ubiquiti’s *original* argument (Synopsis didn’t plead enough facts) is without merit. The novation defense has been adequately and plausibly alleged and Ubiquiti clearly has enough information to contest it.

**C. Failure to Meet Rule 9(b)’s Specificity Requirement**

Ubiquiti moves to dismiss the following affirmative defenses for the failure to plead facts to the required specificity for claims sounding in fraud under Rule 9(b).

**1. Fraud**

In its Fraud Affirmative Defense, Synopsis incorporated the allegations of fraud from its AC, but it also separately identifies eleven affirmative misrepresentations or omissions made by Tsai to Synopsis between October 2013 and May 2014. Amended Answer 5-6. The “heart” of this defense, according to Synopsis’ Opposition, is that Ubiquiti fraudulently induced Synopsis to enter into the MNDA (and other agreements). Oppo. 12-13. Ubiquiti asserts that the allegations of “fraud” against it cannot form a stand-alone defense to its claim that Synopsis breached the MNDA claim, because the MNDA is not specifically mentioned in the fraud affirmative defense averments and is mentioned only in passing in the paragraph 40 of the AC, incorporated by reference. Reply 10-11. Ubiquiti claims that because the affirmative defense itself does not refer to AC ¶ 40 or otherwise itself give notice that the basis of the fraud claim is fraudulent inducement for the MNDA, this affirmative defense is insufficiently pleaded and provides insufficient guidance for Ubiquiti moving forward.

I agree that the fraud affirmative defense could have been more clearly pleaded, but Ubiquiti clearly understands the basis for the defense. That is sufficient.

2. **Unclean Hands**

In its Unclean Hands Affirmative Defense, Synopsys incorporated the allegations from its Amended Complaint, and stated:

Ubiquiti engaged in unjust bad faith conduct that is directly related to the subject matter of the litigation and Ubiquiti's counterclaim by deceiving Synopsys to gain access to its software and by carrying out a scheme to pirate Synopsys' software using counterfeit license keys and unauthorized copies of Synopsys' software. Ubiquiti's bad faith conduct was egregious and caused serious harm to Synopsys.

Amended Answer 6-7. As the alleged deficiencies with this defense are the same as with the fraud affirmative defense that I rejected above, this affirmative defense is sufficiently pleaded.

3. **Estoppel**

In its Estoppel Affirmative Defense, Synopsys incorporated the allegations from its Amended Complaint, and added that:

Ubiquiti's counterclaims are estopped by virtue of its own misconduct, which includes deceiving Synopsys to gain access to its software and using counterfeit license keys to pirate Synopsys software. Ubiquiti knew all material facts about its conduct with respect to its scheme to pirate Synopsys' software and intended for Synopsys to rely on Ubiquiti's conduct and representations. Synopsys was ignorant to the true facts and relied on Ubiquiti's conduct and representations, causing Synopsys prejudice. In addition, Ubiquiti affirmatively represented its assent to the complained of conduct. It would be unjust to award Ubiquiti relief under the circumstances.

Amended Answer 7-8.

Estoppel requires four elements: "(1) the party to be estopped must know the facts; (2) he must intend that his conduct shall be acted on or must so act that the party asserting the estoppel has a right to believe it is so intended; (3) the latter must be ignorant of the true facts; and (4) he must rely on the former's conduct to his injury." *Catch a Wave, Inc. v. Sirius XM Radio, Inc.*, 2013 WL 1996134, at \*3. Synopsys clarifies that this defense is based in part on the same grounds as fraud and in part on the same grounds as waiver (addressed above). As above and for the same reasons as applied to the fraud-based defense, this defense is adequately alleged.

4. **Mistake**

In its Mistake Affirmative Defense, Synopsys incorporated the allegations from its Amended Complaint, and added that:

Ubiquiti’s breach counterclaim is barred by the doctrine of mistake. Synopsys was mistaken about Ubiquiti’s true intent in entering into the underlying agreement because Synopsys believed Ubiquiti was acting in good faith and intended to license Synopsys software. Ubiquiti knew of Synopsys’ mistake because it affirmatively acted to give Synopsys the mistaken impression that Ubiquiti intended to license Synopsys software and comply with all license terms. Synopsys’ mistaken understanding was caused by no fault of Synopsys. Synopsys would not have entered into the agreement but for its mistake.

Amended Answer 8-9. Under California law, “[w]here a mistake of one party at the time a contract was made as to a basic assumption on which he made the contract has a material effect on the agreed exchange of performances that is adverse to him, the contract is voidable by him if he does not bear the risk of the mistake under the rule . . . , and (a) the effect of the mistake is such that enforcement of the contract would be unconscionable, or (b) the other party has reason to know of the mistake or his fault caused the mistake.” *Spitzer v. Aljoe*, No. 13-CV-05442-MEJ, 2016 WL 3279167, at \*10 (N.D. Cal. June 15, 2016) (quoting Restatement (Second) of Contracts § 153). Ubiquiti first argues that because this claim is coextensive with Synopsys’ fraud claim, it fails for the same reasons. However, Synopsys’ fraud affirmative defense has been sufficiently stated and the same is true for mistake.

Ubiquiti also argues that Synopsys has not alleged facts showing that its alleged mistake (not knowing Ubiquiti had no intent to respect the parties’ contractual agreements) had “a material effect on the agreed exchange of performance” in a way that was adverse to Synopsys.<sup>21</sup> However, Synopsys has alleged facts as to how Ubiquiti intended to and did mislead Synopsys, part of which resulted in the signing of the MNDA. As a result, Synopsys relied on the MNDA in providing Ubiquiti access to its software and other resources when it otherwise would not have. Based on the facts alleged in the AC and incorporated into the Amended Answer, this defense has been adequately alleged.

---

<sup>21</sup> In Reply, Ubiquiti argues that Synopsys must also allege facts showing enforcement of the contract would be unconscionable, but Ubiquiti relies on the wrong test. This is not a case of “unilateral mistake,” where one of the parties to the contract “has no reason to know of and does not cause the” other side’s “unilateral mistake of fact.” See *Donovan v. RRL Corp.*, 26 Cal. 4th 261, 282 (2001), as modified (Sept. 12, 2001). Here, Synopsys alleges that Ubiquiti had knowledge of the mistake and/or caused the mistake, therefore, unconscionability need not be alleged.

**D. Unjust Enrichment**

Finally, Ubiquiti moves to strike the “unjust enrichment” affirmative defense, arguing that is it not an affirmative defense, and even if it is, has not been adequately alleged because: (i) none of Synopsys’ other equitable defenses have been adequately alleged; (ii) Synopsys fails to allege how permitting recovery by Ubiquiti on its breach of MNDA claim would be unjust; and (iii) Synopsys fails to allege any connection between Ubiquiti’s alleged piracy and the breach of the MNDA. Mot. 17-18. In its Amended Answer, Synopsys alleges the following:

Synopsys incorporates the factual allegations set forth above and the factual allegations of its Amended Complaint, including without limitation paragraphs 1 through 66. Ubiquiti has been unjustly enriched by its piracy of Synopsys’ software and is therefore estopped from seeking any recovery. Ubiquiti pirated Synopsys’ software to avoid paying millions of dollars-worth of license fees to Synopsys. It would be unjust for Ubiquiti to retain the benefits of that piracy or to obtain any relief on its counterclaims.

Amended Answer 8.

As an initial matter, the California Supreme Court recently confirmed that unjust enrichment can be a stand-alone cause of action. *See Bruton v. Gerber Prod. Co.*, No. 15-15174, 2017 WL 1396221, at \*1 (9th Cir. Apr. 19, 2017) (relying on *Hartford Cas. Ins. Co. v. J.R. Mktg., L.L.C.*, 61 Cal.4th 988, 1000 (2015)). In addition, as discussed above, Synopsys’ equitable defenses have been adequately alleged. As to the specifics of why preventing Ubiquiti from recovering on its breach claim would be unjust, the allegations are adequate. Ubiquiti understands exactly why Synopsys thinks it would be unjust for Ubiquiti to receive or retain damages (if any) from Synopsys for the alleged breach of contract if Synopsys proves its piracy claims. I will not strike this defense.

Ubiquiti’s motion to strike is DENIED.

**III. UNIL MOTION TO DISMISS**

**A. Motion to Dismiss for Lack of Personal Jurisdiction**

UNIL moves to dismiss, arguing that there is no basis for general or specific jurisdiction over it with respect to the claims made by Synopsys. Dkt. No. 35. In Opposition, Synopsys relies on specific, not general, jurisdiction. It asserts that by illegally downloading the software and user materials from its websites located in California (or in one instance, in Ireland but through a host

located in California), UNIL has not only expressly agreed to venue here but has also purposefully directed its illegal conduct and performed some of that conduct in California.

### 1. Legal Standard

For the exercise of personal jurisdiction over a defendant, due process requires that the defendant “have certain minimum contacts” with the forum state “such that the maintenance of the suit does not offend ‘traditional notions of fair play and substantial justice.’” *Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

In the Ninth Circuit, there is a three-prong test for analyzing a claim of specific personal jurisdiction: (1) the non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim must be one which arises out of or relates to the defendant’s forum-related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice, in other words, be reasonable. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004). The “purposeful availment analysis is most often used in suits sounding in contract. . . . A purposeful direction analysis, on the other hand, is most often used in suits sounding in tort.” *Id.*

As both sides point out, under the second prong, the Supreme Court recently clarified that “[f]or a State to exercise jurisdiction consistent with due process, the defendant’s suit-related conduct must create a substantial connection with the forum State.” *Walden v. Fiore*, 134 S. Ct. 1115, 1121 (2014). That occurs where, first, the relationship “arise[s] out of contacts that the ‘defendant himself’ creates with the forum State.” *Id.* at 1122. Second, the “minimum contacts” analysis “looks to the defendant’s contacts with the forum State itself, not the defendant’s contacts with persons who reside there.” *Id.* The concern, especially with respect to the second factor, is to hail a defendant “into court in a forum State based on his own affiliation with the State, not based on the ‘random, fortuitous, or attenuated’ contacts he makes by interacting with other persons affiliated with the State.” *Id.* at 1123.



2. **UNIL's Contacts with California**

As alleged, UNIL's connections with and activities directed at California include:

- Tsai, while physically located in California, began negotiating with Synopsys for evaluation access to its software for evaluations to be done in Taiwan. AC ¶ 49. Tsai admits his initial contact was with Bergman in California, with UNIL employees copied on those emails. According to Tsai, the subsequent contacts were with Huang, whom Tsai believes is associated with Synopsys Taiwan. Tsai Decl. ¶ 6.
- Tsai continued the negotiations on behalf of UNIL, attending an in-person meeting in Taiwan. AC ¶ 50. Tsai asserts that the only Synopsys employees involved in that meeting were Synopsys Taiwan employees. Tsai Decl. ¶¶ 9-10.
- The software and documentation UNIL downloaded on April 16, 2014 – as a result of Tsai's negotiations – came from servers in California, and the software downloaded by UNIL on May 19, 2014 came via a remote host located in California. AC ¶¶ 53, 56. Synopsys alleges that UNIL and the other defendants continued to access Synopsys' California-based websites after that time. *Id.* ¶ 56.
- Synopsys alleges that in order to download that materials at issue, the user would have had to agree to terms of use, which contain choice of law and venue provisions consenting to jurisdiction in this Court. AC ¶ 17. Tsai does not indicate who downloaded the software on behalf of UNIL, limiting his declaration to his initial download of the VCS software on behalf of Ubiquiti. Tsai Decl. ¶ 11.
- Ubiquiti and UNIL used the same "virtual machines" to run unauthorized copies of Synopsys' software using counterfeit license keys, and some of these machines were located in California. AC ¶ 62.
- Using Ubiquiti and UNIL's shared IT infrastructure, UNIL transmitted counterfeit keys and key generation tools to Ubiquiti in California. AC ¶¶ 57-58.

a. **Terms of Use**

Synopsys argues first that through accessing Synopsys' customer support and download websites (hosted physically in or remotely through California), UNIL necessarily agreed to

Synopsys' venue selection clause placing jurisdiction in this Court. Oppo. 6-7; AC ¶ 17.

In Reply, UNIL relies on the Tsai declaration stating that when he downloaded software for Ubiquiti in late 2013, he did not recall agreeing to terms of use. Reply 2; Tsai Decl. ¶ 11. However, Tsai is not exactly adamant about *not* agreeing to any terms of use. Instead, he simply cannot recall that he did. Moreover, Tsai does not address who at UNIL downloaded the software and other documentation in April and May 2014. Nor does Tsai address any use of Synopsys' websites after that time, despite Synopsys' allegations that UNIL and the other defendants continued to access Synopsys' websites in conjunction with their use of the software downloaded in April and May 2014. Instead of providing fact testimony to counter Synopsys' allegations, UNIL argues that because Tsai didn't see any or remember agreeing to any terms of use, there must have been none and that "would have been true" at the time unidentified users at UNIL downloaded Synopsys' files "in that same time period." Reply 3.

UNIL attempts to skip over the gaps in Tsai's declaration, arguing that it needn't come forward with facts because the initial burden is on Synopsys to present affirmative proof that a UNIL user "clicked through" and affirmatively agreed to their terms of use as of a specific date. Reply 2. UNIL points out that in its Opposition, Synopsys may have undercut its own argument by seemingly admitting that the venue selection clause may not have been in place prior to November 24, 2014. Oppo. 6 ("The evidence will show that UNIL assented to jurisdiction at least by accessing Synopsys' customer support and file download websites after November 24, 2014, thereby agreeing to terms of use . . . ."). However, Synopsys has *also* alleged that UNIL and the other defendants "continued" to access Synopsys websites after the May 2014 download. Oppo. 6-7.

On this record, UNIL has not shown why Synopsys' allegations of UNIL's agreement to Synopsys' terms of use does not weigh strongly in favor of jurisdiction over UNIL.

**b. Purposeful Direction**

Even if UNIL was correct and neither Tsai nor anyone else at UNIL agreed to Synopsys' terms of use, there are still sufficient allegations of purposeful direction to support jurisdiction over UNIL. Synopsys points to the following: (i) UNIL's uncontested downloading of software

from servers located in California, where Synopsys is headquartered; (ii) allegations that UNIL transmitted counterfeit and illicit license keys as well as unauthorized copies of software to California-based Ubiquiti; (iii) UNIL is associated with virtual machines that used counterfeit license keys within California; and (iv) a UNIL employee contacted Synopsys’ U.S.-based customer service support personnel to obtain assistance. These intentional acts, according to Synopsys, demonstrate that UNIL purposefully aimed its conduct to California. Oppo 8-9.

As to the first acts of downloading, UNIL argues that Synopsys has failed to “prove” that any UNIL employees knew Synopsys had servers in California. It relies exclusively on Tsai’s Reply Declaration where Tsai –who again expressly disclaims being a UNIL employee, yet is testifying on behalf of what UNIL did and knew – says that in his experience “a user of a company’s file download website may not know where that company’s computer servers are located.” Tsai Reply Decl. ¶ 5. Synopsys points out that at this juncture it cannot disprove what UNIL employees actually knew, but that it has presented detailed allegations regarding Synopsys being headquartered in California and UNIL’s knowledge of the same given its experience in the industry. I agree that those allegations make it sufficiently plausible to infer knowledge or reckless disregard on the part of UNIL. *See Walden*, 688 F.3d at 575 (“We will draw reasonable inferences from the complaint in favor of the plaintiff where personal jurisdiction is at stake, and will assume credibility.”).

Synopsys also relies on decisions that have found that there were sufficient contacts where defendants access intellectual property on servers within the forum state. For example, in *Microsoft Corp. v. Mountain W. Computers, Inc.*, No. C14-1772RSM, 2015 WL 4479490 (W.D. Wash. July 22, 2015), the district court (following *Walden*) held that where “[d]efendants affirmatively contacted Microsoft through internet contact with its servers and by telephone to validate the software it was installing,” that was sufficient “express aiming,” regardless of “whether Defendants knew where Plaintiff’s servers were located” because defendants “admit that they knew Microsoft is located in Washington.” *Id.* at \*7; *see also Gen. Motors L.L.C. v. Autel. US Inc.*, No. 14-14864, 2016 WL 1223357, at \*4 (E.D. Mich. Mar. 29, 2016) (“that Autel ITC has reached into Michigan to access GM’s intellectual property located on its servers residing in

Michigan. . . . This is an example of purposeful availment.”); *see also Autodesk, Inc. v. Kobayashi + Zedda Architects Ltd.*, 191 F. Supp. 3d 1007, 1018 (N.D. Cal. 2016) (“Defendant’s alleged copying of Plaintiff’s software purportedly caused Plaintiff injury in California, and this particular injury would not have occurred ‘but for’ Defendant’s alleged infringing conduct.”).

UNIL attempts to distinguish the *Microsoft* case by arguing that in that case there were allegations there that the defendant entered an unauthorized key on Microsoft’s computer server in Washington to unlock a security feature, but here Synopsys gave UNIL permission to download the software in April/May 2014. That is true, but it ignores Synopsys’ allegations that Synopsys would not have given UNIL that permission but for UNIL’s fraudulent representations about its intentions. As discussed above, Synopsys’ fraud-based allegations are sufficient and plausible. The Amended Complaint identifies the fraudulent statements that convinced Synopsys to provide UNIL access to the software actually or virtually hosted on Synopsys’ California servers. That those statements were made by Tsai, acting on behalf of UNIL and allegedly with the knowledge of, if not the participation of, UNIL employees. UNIL does not dispute that because of representations made by Tsai and the other UNIL employees at the Taipei in-person meeting, UNIL secured access to and downloaded Synopsys’ software that was hosted physically or virtually on California-based servers.<sup>22</sup>

As to the second and third acts, UNIL presents no evidence *from a UNIL employee* to counter or raise an issue as to whether UNIL transmitted counterfeit and illegal license keys or unauthorized software to Ubiquiti, or dispute that UNIL is associated with virtual machines that used counterfeit license keys in California. Instead, UNIL relies on the Tsai and Wang Reply declarations that state “to their knowledge,” as the only Ubiquiti employees who worked with UNIL employees on semiconductor chip design activities, no UNIL employee transmitted to any Ubiquiti employee “in California” unauthorized license keys or unauthorized copies of software.

---

<sup>22</sup> UNIL appears to argue that because the in-person Taipei meeting was held with individuals Tsai believes are employees of Synopsys Taiwan – assertions that Synopsys objects to, although substantiated in part in Tsai’s Reply Declaration – there can be no fraud directed at California. However, *neither* Tsai *nor* any UNIL employee declares that UNIL believed it was securing the software from Synopsys Taiwan or that it was downloading the software from Synopsys Taiwan.

Tsai Reply Decl. ¶¶ 2-3, Wang Decl. ¶¶ 2-3. However, these declarations are from Ubiquiti employees, not UNIL employees, and made only to the best of their knowledge. More fundamentally, these assertions go to the *heart* of this case. UNIL cites no case law allowing a defendant to avoid personal subject matter jurisdiction based on factual assertions that contradict the heart and theory of the plaintiff’s complaint. “They did not do it” because I would have known about it will not suffice.

Finally, UNIL does not address Synopsys’ allegations that Ubiquiti and UNIL share IT infrastructure and it appears that UNIL and the other Enterprise members are “associated” with virtual machines that used counterfeit license keys within California. AC ¶¶ 62, 133. Instead, UNIL argues that Synopsys’ allegations are insufficient because Synopsys fails to identify with specificity the acts UNIL separately took in California that would support specific jurisdiction on this basis. Reply 7 (citing AC ¶ 62). However, UNIL had the opportunity to contradict Synopsys’ allegations about its IT infrastructure and the acts but failed to do so. Further specificity will be provided by Synopsys through discovery as the case progresses.

As to the fourth alleged intentional act – UNIL’s communications with California-based Synopsys support personal – UNIL argues that the U.S.-based employee at issue was in Taiwan when UNIL communicated with him. Tsai Decl. ¶ 12. I agree that if this was the only express fact relied on by Synopsys, it would be insufficient. *See, e.g., Walden*, 134 S. Ct. at 1122 (“[O]ur ‘minimum contacts’ analysis looks to the defendant’s contacts with the forum State itself, not the defendant’s contacts with persons who reside there.”). But this is not the only jurisdictional fact alleged. The others are more than sufficient to demonstrate that UNIL’s intents with and connections to California were far more than “random, fortuitous, or attenuated.” *Id.* at 1123.<sup>23</sup>

#### **B. Motion to Dismiss for Failure to State a Claim**

UNIL incorporates and reasserts the arguments made by Ubiquiti addressed above on

---

<sup>23</sup> As noted above, in addition to an analysis of purposeful direction and defendant’s forum-related contacts, courts also consider whether exercise of jurisdiction is reasonable. In its Motion, UNIL expressly and knowingly failed to raise an argument as to reasonableness of exercising jurisdiction. UNIL MTD at 7 n.3. Having presented no argument on the point, I will not consider it, but note that given the facts alleged and UNIL’s relationship to Ubiquiti, exercise of jurisdiction over it in this forum is not unreasonable.

Ubiquiti and Tsai's motion to dismiss under Rule 12(b)(6). UNIL makes an additional, separate argument that because there are no allegations that UNIL *used* any counterfeit license keys or infringed any copyrights *within the United States*, there is no liability under the DMCA or civil RICO for its wholly extraterritorial conduct. I disagree. The Amended Complaint is replete with allegations that UNIL accessed through fraud Synopsys' software stored on servers in the United States (or through a virtual host located in California). There are also adequate allegations that UNIL had connections to virtual machines running in California using counterfeit keys and running unauthorized software. *See* AC ¶¶ 28, 52-56, 62.

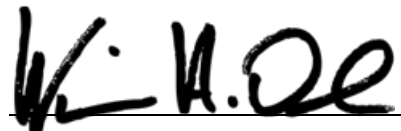
UNIL's motion to dismiss for lack of jurisdiction and for failure to state a claim is DENIED.

### CONCLUSION

For the foregoing reasons, Ubiquiti and Tsai's motion to dismiss is GRANTED in limited part with respect to the Anti-Counterfeiting Act claim, and as to some of the predicate acts under RICO. Ubiquiti and Tsai's motion to strike the affirmative defenses is DENIED. UNIL's motion to dismiss for lack of jurisdiction is DENIED. If Synopsys wishes to file a further Amended Complaint, it must do so within twenty (20) days of the date of this Order.

**IT IS SO ORDERED.**

Dated: August 15, 2017



William H. Orrick  
United States District Judge